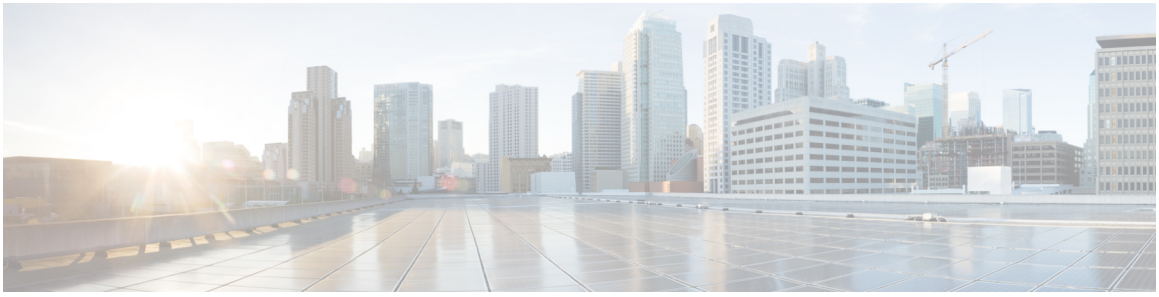
Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E

First Published: 2014-12-19

Last Modified: 2018-07-05

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

Preface

Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in **bold** font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`Courier` font	Terminal sessions and information the system displays appear in `courier` font.
`Bold Courier` font	**`Bold Courier`** font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
{x | y}	Required alternative keywords are grouped in braces and separated by vertical bars.

Convention	Description
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document may use the following conventions for reader alerts:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information will help you solve a problem.*

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time.* You can save time by performing the action described in the paragraph.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Related Documentation

Note Before installing or upgrading the switch, refer to the switch release notes.

- Cisco Catalyst 3850 Series Switches documentation, located at:

  http://www.cisco.com/go/cat3850_docs

- Cisco SFP, SFP+, and QSFP+ modules documentation, including compatibility matrixes, located at:

  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html

- Cisco Validated Designs documents, located at:

  http://www.cisco.com/go/designzone

Obtaining Documentation and Submitting a Service Request

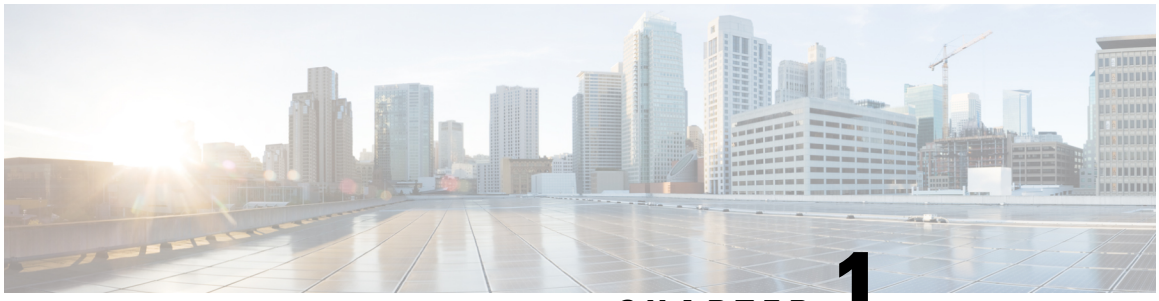
For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

PART I

CleanAir



CHAPTER 1

Configuring Cisco CleanAir

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for CleanAir

You can configure Cisco CleanAir only on CleanAir-enabled access points.

Only Cisco CleanAir-enabled access points using the following access point modes can perform Cisco CleanAir spectrum monitoring:

- Local—In this mode, each Cisco CleanAir-enabled access point radio provides air quality and interference detection reports for the current operating channel only.
- Monitor—When Cisco CleanAir is enabled in monitor mode, the access point provides air quality and interference detection reports for all monitored channels.

  The following options are available:

- All— All channels
- DCA—Channel selection governed by the DCA list
- Country—All channel legal within a regulatory domain

Note The access point does not participate in AQ HeatMap in Prime Infrastructure.

- SE-Connect—This mode enables a user to connect a Spectrum Expert application running on an external Microsoft Windows XP or Vista PC to a Cisco CleanAir-enabled access point in order to display and analyze detailed spectrum data. The Spectrum Expert application connects directly to the access point, bypassing the switch. An access point in SE-Connect mode does not provide any Wi-Fi, RF, or spectrum data to the switch. All CleanAir system functionality is suspended while the AP is in this mode, and no clients are served. This mode is intended for remote troubleshooting only. Up to three active Spectrum Expert connections are possible.
- Only Cisco Catalyst 3850 and Switches can function as a Mobility Agent.
- Cisco Catalyst 3850 Switches and Cisco 5760 Wireless LAN Controllers can function as Mobility Controllers.

Related Topics

Enabling CleanAir for 2.4-GHz Band, on page 8
Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices, on page 9
Configuring Interference Reporting for 2.4-GHz Devices, on page 10
Enabling CleanAir for 5-GHz Band, on page 12
Configuring a CleanAir Alarm for 5-GHz Air-Quality and Devices, on page 12
Configuring Interference Reporting for 5-GHz devices, on page 13

Restrictions on CleanAir

- Access points in monitor mode do not transmit Wi-Fi traffic or 802.11 packets. They are excluded from radio resource management (RRM) planning and are not included in the neighbor access point list. IDR clustering depends on the switch's ability to detect neighboring in-network access points. Correlating interference device detections from multiple access points is limited between monitor-mode access points.
- SE-connect is an access point mode similar to local mode or monitor mode. The access point provides spectrum information to Spectrum Expert only for the current channel(s). The spectrum data is available for the current active channel(s) and the common monitored channel list is available. The access point continues to send AQ (Air Quality) and IDR (Interference Device Reports) reports to the switch and perform normal activities according to the current mode. Sniffer and rogue detections access point modes are incompatible with all types of CleanAir spectrum monitoring.
- Local Mode access point—Serves WLAN clients with the time slicing off-channel scanning and listens for 50 ms on each channel, and scans configurable feature scanning for all/country/DCA channels.
- Monitor Mode access point—Does not serve WLAN clients and are dedicated to scanning only. These access points listen for 1.2 s on each channel, and scans all channels.

- Monitor Mode access point in slot 2 operates at 2.4 GHz only.
- Cisco recommends a ratio of 1 monitor mode access point for every 5 local mode access points, this may also vary based on the network design and expert guidance for best coverage.
- Spectrum Expert (Windows XP laptop client) and AP should be pingable, otherwise; it will not work.

Related Topics

Enabling CleanAir for 2.4-GHz Band, on page 8
Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices, on page 9
Configuring Interference Reporting for 2.4-GHz Devices, on page 10
Enabling CleanAir for 5-GHz Band, on page 12
Configuring a CleanAir Alarm for 5-GHz Air-Quality and Devices, on page 12
Configuring Interference Reporting for 5-GHz devices, on page 13

Information About CleanAir

Cisco CleanAir is a spectrum intelligence solution designed to proactively manage the challenges of a shared wireless spectrum. It allows you to see all of the users of the shared spectrum (both native devices and foreign interferers). It also enables the network to act upon this information. For example, you could manually remove the interfering device, or the system could automatically change the channel away from the interference. CleanAir provides spectrum management and RF visibility.

A Cisco CleanAir system consists of CleanAir-enabled access points, Cisco Wireless LAN Controllers, and Cisco Prime Infrastructure. These access points collect information about all devices that operate in the industrial, scientific, and medical (ISM) bands, identify and evaluate the information as a potential interference source, and forward it to the Cisco WLC. The Cisco WLC controls the access points, collects spectrum data, and forwards information to Cisco Prime Infrastructure or a Cisco mobility services engine (MSE) upon request.

Any networking configurations can be performed only on the mobility controller, configurations cannot be performed in the MA mode. However, any radio level CleanAir configurations can be done using mobility anchor.

For every device operating in the unlicensed band, Cisco CleanAir tells what it is, where it is, how it is impacting your wireless network, and what actions you or your network should take. It simplifies RF.

Wireless LAN systems operate in unlicensed 2.4-GHz and 5-GHz ISM bands. Many devices, such as microwave ovens, cordless phones, and Bluetooth devices also operate in these bands and can negatively affect the Wi-Fi operations.

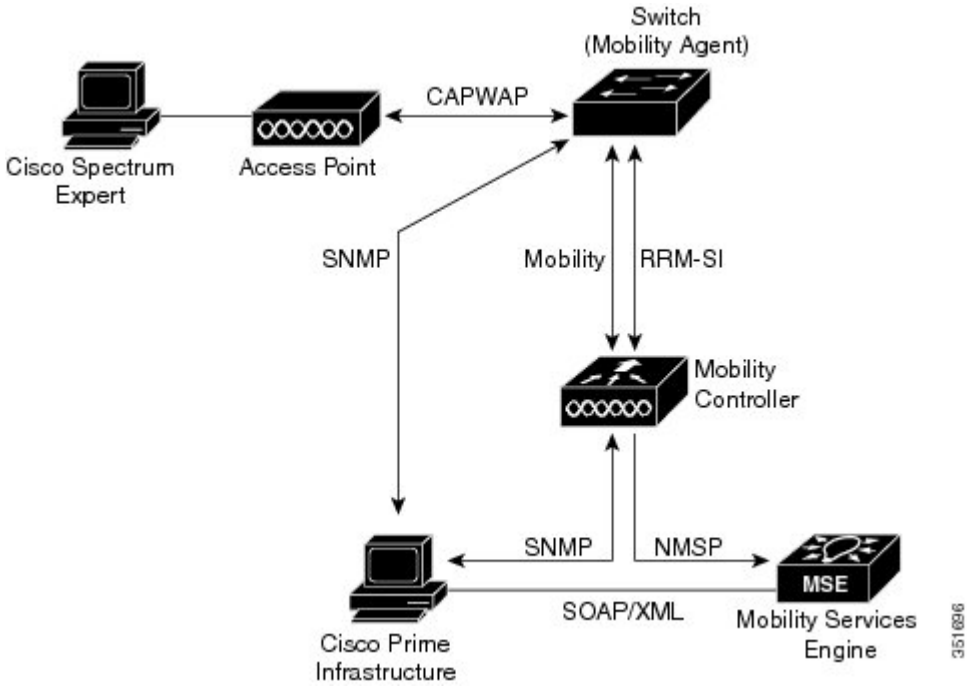
Some of the most advanced WLAN services, such as voice over wireless and IEEE 802.11n radio communications, could be significantly impaired by the interference caused by other legal users of the ISM bands. The integration of Cisco CleanAir functionality addresses this problem of radio frequency (RF) interference.

Cisco CleanAir Components

The basic Cisco CleanAir architecture consists of Cisco CleanAir-enabled APs and switch. Cisco Prime Infrastructure (PI), Mobility Services Engine (MSE) and Cisco Spectrum Expert are optional system

components. Cisco PI and MSE provide user interfaces for advanced spectrum capabilities such as historic charts, tracking interference devices, location services and impact analysis.

Figure 1: Cisco CleanAir Solution



An access point equipped with Cisco CleanAir technology collects information about non-Wi-Fi interference sources, processes it, and forwards it to the MA. The access point sends AQR and IDR reports to the controller.

The mobility controller (MC) controls and configures CleanAir-capable access points, collects and processes spectrum data, and provides it to the PI and/or the MSE. The MC provides local user interfaces (GUI and CLI) to configure basic CleanAir features and services and display current spectrum information. The MC also does detection, merging and mitigation of interference devices using RRM TPC and DCM. For details, see Interference Device Merging.

Cisco PI provides advanced user interfaces for CleanAir that include feature enabling and configuration, consolidated display information, historic AQ records and reporting engines. PI also shows charts of interference devices, AQ trends, and alerts.

Cisco MSE is required for location and historic tracking of interference devices, and provides coordination and consolidation of interference reports across multiple controllers. MSE also provides adaptive Wireless Intrusion Prevention System (WIPS) service that provides comprehensive over-the-air threat detection, location and mitigation. MSE also merges all the interference data.

To obtain detailed spectrum data that can be used to generate RF analysis plots similar to those provided by a spectrum analyzer, you can configure a Cisco CleanAir-enabled access point to connect directly to a Microsoft Windows XP or Vista PC running the Cisco Spectrum Expert application.

The switch performs the following tasks in a Cisco CleanAir system:

- Configures Cisco CleanAir capabilities on the access point.
- Provides interfaces (GUI, CLI, and SNMP) for configuring Cisco CleanAir features and retrieving data.
- Displays spectrum data.

- Collects and processes AQRs from the access point and stores them in the air quality database. AQRs contains information about the total interference from all identified sources represented by Air Quality Index (AQI) and summary for the most severe interference categories. The CleanAir system can also include unclassified interference information under per interference type reports which enable you to take action in cases where the interference due to unclassified interfering devices is more.
- Collects and processes Interference Device Reports (IDRs) from the access point and stores them in the interference device database.
- Forwards spectrum data to Prime Infrastructure and the MSE.

Terms Used in Cisco CleanAir

Table 1: CleanAir-related Terms

Term	Decription
AQI	Air Quality Index. The AQI is an indicator of air quality, based on the air pollutants. An AQI of 0 is bad and an AQI > 85 is good.
AQR	Air Quality Report. AQRs contain information about the total interference from all identified sources represented by AQI and summary of the most severe interference categories. AQRs are sent every 15 minutes to the Mobility Controller and every 30 seconds in the Rapid mode.
DC	Duty Cycle. Percentage of time that the channel is utilized by a device.
EDRRM	EDRRM Event Driven RRM. EDRRM allows an access point in distress to bypass normal RRM intervals and immediately change channels.
IDR	Interference Device Reports that the access point sends to the controller.
ISI	Interference Severity Index. The ISI is an indicator of the severity of the interference.
MA	Mobility Agent. An MA is either an access switch that has a wireless module running on it or an MC with an internal MA running on it. An MA is the wireless component that maintains client mobility state machine for a mobile client that is connected to an access point to the device that the MA is running on.
MC	Mobility Controller. An MC provides mobility management services for inter-peer group roaming events. The MC provides a central point of contact for management and sends the configuration to all the mobility agents under its sub-domain of their mobility configuration, peer group membership and list of members.
RSSI	Received Signal Strength Indicator. RSSI is a measurement of the power present in a received radio signal. It is the power at which an access point sees the interferer device.

Interference Types that Cisco CleanAir can Detect

Cisco CleanAir can detect interference, report on the location and severity of the interference, and recommend different mitigation strategies. Two such mitigation strategies are persistent device avoidance and spectrum event-driven RRM.

Wi-Fi chip-based RF management systems share these characteristics:

- Any RF energy that cannot be identified as a Wi-Fi signal is reported as noise.

- Noise measurements that are used to assign a channel plan tend to be averaged over a period of time to avoid instability or rapid changes that can be disruptive to certain client devices.
- Averaging measurements reduces the resolution of the measurement. As such, a signal that disrupts clients might not look like it needs to be mitigated after averaging.
- All RF management systems available today are reactive in nature.

Cisco CleanAir is different and can positively identify not only the source of the noise but also its location and potential impact to a WLAN. Having this information allows you to consider the noise within the context of the network and make intelligent and, where possible, proactive decisions. For CleanAir, two types of interference events are common:

- Persistent interference
- Spontaneous interference

Persistent interference events are created by devices that are stationary in nature and have intermittent but largely repeatable patterns of interference. For example, consider the case of a microwave oven located in a break room. Such a device might be active for only 1 or 2 minutes at a time. When operating, however, it can be disruptive to the performance of the wireless network and associated clients. Using Cisco CleanAir, you can positively identify the device as a microwave oven rather than indiscriminate noise. You can also determine exactly which part of the band is affected by the device, and because you can locate it, you can understand which access points are most severely affected. You can then use this information to direct RRM in selecting a channel plan that avoids this source of interference for the access points within its range. Because this interference is not active for a large portion of the day, existing RF management applications might attempt to again change the channels of the affected access points. Persistent device avoidance is unique, however, in that it remains in effect as long as the source of interference is periodically detected to refresh the persistent status. The Cisco CleanAir system knows that the microwave oven exists and includes it in all future planning. If you move either the microwave oven or the surrounding access points, the algorithm updates RRM automatically.

Note Spectrum event-driven RRM can be triggered only by Cisco CleanAir-enabled access points in local mode.

Note All the APs using qualcomm atheros chipset sends air-quality as 100 percent even if the radios detect interference.

Spontaneous interference is interference that appears suddenly on a network, perhaps jamming a channel or a range of channels completely. The Cisco CleanAir spectrum event-driven RRM feature allows you to set a threshold for air quality (AQ) that, if exceeded, triggers an immediate channel change for the affected access point. Most RF management systems can avoid interference, but this information takes time to propagate through the system. Cisco CleanAir relies on AQ measurements to continuously evaluate the spectrum and can trigger a move within 30 seconds. For example, if an access point detects interference from a video camera, it can recover by changing channels within 30 seconds of the camera becoming active. Cisco CleanAir also identifies and locates the source of interference so that more permanent mitigation of the device can be performed at a later time.

In the case of Bluetooth devices, Cisco CleanAir-enabled access points can detect and report interference only if the devices are actively transmitting. Bluetooth devices have extensive power save modes. For example, interference can be detected when data or voice is being streamed between the connected devices.

Interference Device Merging

The Interference Devices (ID) messages are processed on a Mobility Controller (MC). The Mobility Anchor (MA) forwards the ID messages from APs and hence they are processed on the MC. The MC has visibility of the neighbor information across APs connected to different MAs.

ID merging logic requires AP neighbor information. Neighbor information is obtained from the RRM module. This api only gives neighbor information to the APs directly connected to MC.

Currently the AP neighbor list on MA is synced to MC once every 3 minutes; hence the AP neighbor list obtained by this api could be at most 3 mins old. This delay results in delay in merging of Devices as they are discovered. The subsequent periodic merge will pick up the updated neighbor information and merge is performed

Persistent Devices

Some interference devices such as outdoor bridges and Microwave Ovens only transmit when needed. These devices can cause significant interference to the local WLAN due to short duration and periodic operation remain largely undetected by normal RF management metrics. With CleanAir the RRM DCA algorithm can detect, measure, register and remember the impact and adjust the DCA algorithm. This minimizes the use of channels affected by the persistent devices in the channel plan local to the interference source. Cisco CleanAir detects and stores the persistent device information in the switch and this information is used to mitigate interfering channels.

Persistent Devices Detection

CleanAir-capable Monitor Mode access point collects information about persistent devices on all configured channels and store the information in controller. Local/Bridge mode AP detects interference devices on the serving channels only.

Persistent Device Avoidance

When a Persistent Device (PD) is detected in the CleanAir module, it is reported to the RRM module on the MA. This information is used in the channel selection by the subsequent EDRRM Event Driven RRM (ED-RRM) signal sent to the RRM module.

EDRRM and AQR Update Mode

EDRRM is a feature that allows an access point that is in distress to bypass normal RRM intervals and immediately change channels. A CleanAir access point always monitors AQ and reports the AQ every 15 minutes. AQ only reports classified interference devices. The key benefit of EDRRM is very fast action time. If an interfering device is operating on an active channel and causes enough AQ degradation to trigger an EDRRM, then no clients will be able to use that channel or the access point. You must remove the access point from the channel. EDRRM is not enabled by default, you must first enable CleanAir and then enable EDRRM.

AQRs are only available on the MC. The mode configuration and timers are held in Radio Control Block (RCB) on MA (for APs connected to MA). There is no change to the current API available for EMS/NMS. No change is required for directly connected APs as RCB (spectrum config and timers) is available locally. For remote APs (APs connected to MA), three new control messages are added. These three messages are for enable, restart timer and disable rapid update mode for a given AP MAC address and slot.

Related Topics

Configuring EDRRM for CleanAir-Events, on page 15

CleanAir High Availability

CleanAir configuration (network and radio) is stateful during the switchover. On the MC, Embedded Instrumentation Core (EICORE) provides the sync on network configurations across active and standby nodes. The radio configurations are synced using the HA Infrastructure. The CleanAir configurations on MA are pulled from the MC upon joining. The network configuration is not stored in the EICORE on MA, hence it is synced using HA Infrastructure.

CleanAir Data (AQ and IDR) reports are not stateful, that is, the standby and active nodes are not synced. On switchover, the APs send the reports to the current active slot. The RRM Client (HA Infra Client) is used for CleanAir HA sync.

How to Configure CleanAir

Enabling CleanAir for 2.4-GHz Band

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 2	**ap dot11 24ghz cleanair**
	Example:
	`Switch(config)#ap dot11 24ghz cleanair`
	`Switch(config)#no ap dot11 24ghz cleanair`
		Enables the CleanAir feature on 802.11b network. Add **no** in the command to disable CleanAir on the 802.11b network.

Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for CleanAir, on page 1

Restrictions on CleanAir, on page 2
CleanAir FAQs, on page 26

Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz cleanair alarm air-quality threshold** *threshold_value* **Example:** `Switch(config)#ap dot11 24ghz cleanair alarm air-quality threshold 50`	Configures the alarm for the threshold value for air-quality for all the 2.4-GHz devices. Add the **no** form of this command to disable the alarm.
Step 3	**ap dot11 24ghz cleanair alarm device** {**bt-discovery** | **bt-link** | **canopy** | **cont-tx** | **dect-like** | **fh** | **inv** | **jammer** | **mw-oven** | **nonstd** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile** | **xbox** | **zigbee** } **Example:** `Switch(config)#ap dot11 24ghz cleanair alarm device canopy`	Configures the alarm for the 2.4-GHz devices. Add the **no** form command to disable the alarm. • **bt-discovery**—Bluetooth Discovery. • **bt-link**—Bluetooth Link. • **canopy**—Canopy devices. • **cont-tx**—Continuous Transmitter. • **dect-like**—Digital Enhanced Cordless Communication (DECT)-like phone. • **fh**—802.11 frequency hopping devices. • **inv**—Devices using spectrally inverted WiFi signals. • **jammer**—Jammer. • **mw-oven**—Microwave oven. • **nonstd**—Devices using non standard Wi-Fi channels. • **report**—Interference device reporting. • **superag**—802.11 SuperAG devices. • **tdd-tx**—TDD Transmitter. • **video**—Video cameras. • **wimax-fixed**—WiMax Fixed.

	Command or Action	Purpose
		• **wimax-mobile**—WiMax Mobile. • **xbox**—Xbox. • **zigbee**—802.15.4 devices.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for CleanAir, on page 1
Restrictions on CleanAir, on page 2
CleanAir FAQs, on page 26

Configuring Interference Reporting for 2.4-GHz Devices

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 2	**ap dot11 24ghz cleanair device** {**bt-discovery** | **bt-link** | **canopy** | **cont-tx** | **dect-like** | **fh** | **inv** | **jammer** | **mw-oven** | **nonstd** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile** | **xbox** | **zigbee** }
	Example:
	`Switch(config)# ap dot11 24ghz cleanair device bt-discovery`
	`Switch(config)# ap dot11 24ghz cleanair device bt-link`
	`Switch(config)# ap dot11 24ghz cleanair device canopy`
	`Switch(config)# ap dot11 24ghz cleanair device cont-tx`
	`Switch(config)# ap dot11 24ghz cleanair device dect-like`
	`Switch(config)# ap dot11 24ghz cleanair device fh`
		Configures the 2.4 GHz interference devices to report to the switch. Use the **no** form of this command to disable the configuration.
		• **bt-discovery**—Bluetooth Discovery
		• **bt-link**—Bluetooth Link
		• **canopy**—Canopy devices
		• **cont-tx**- Continuous Transmitter
		• **dect-like**- Digital Enhanced Cordless Communication (DECT) like phone
		• **fh**- 802.11 frequency hopping devices
		• **inv**- Devices using spectrally inverted WiFi signals
		• **jammer**- Jammer
		• **mw-oven**- Microwave Oven
		• **nonstd**- Devices using non-standard WiFi channels

	Command or Action	Purpose
	Switch(config)# **ap dot11 24ghz cleanair device inv** Switch(config)# **ap dot11 24ghz cleanair device jammer** Switch(config)# **ap dot11 24ghz cleanair device mw-oven** Switch(config)# **ap dot11 24ghz cleanair device nonstd** Switch(config)# **ap dot11 24ghz cleanair device report** Switch(config)# **ap dot11 24ghz cleanair device superag** Switch(config)# **ap dot11 24ghz cleanair device tdd-tx** Switch(config)# **ap dot11 24ghz cleanair device video** Switch(config)# **ap dot11 24ghz cleanair device wimax-fixed** Switch(config)# **ap dot11 24ghz cleanair device wimax-mobile** Switch(config)# **ap dot11 24ghz cleanair device xbox** Switch(config)# **ap dot11 24ghz cleanair device zigbee**	• **report**- no description • **superag**- 802.11 SuperAG devices • **tdd-tx**- TDD Transmitter • **video**- Video cameras • **wimax-fixed**- WiMax Fixed • **wimax-mobile**- WiMax Mobile • **xbox**- Xbox • **zigbee**- 802.15.4 devices
Step 3	**end** **Example:** Switch(config)# **end**	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for CleanAir, on page 1
Restrictions on CleanAir, on page 2
CleanAir FAQs, on page 26
Monitoring the Interference Devices (GUI), on page 24

Enabling CleanAir for 5-GHz Band

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 2	**ap dot11 5ghz cleanair**
	Example:
	`Switch(config)#ap dot11 5ghz cleanair`
	`Switch(config)#no ap dot11 5ghz cleanair`
		Enables the CleanAir feature on 802.11a network. Add **no** in the command to disable CleanAir on the 802.11a network.

Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for CleanAir, on page 1
Restrictions on CleanAir, on page 2
CleanAir FAQs, on page 26

Configuring a CleanAir Alarm for 5-GHz Air-Quality and Devices

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 5ghz cleanair alarm air-quality threshold** *threshold_value* **Example:** `Switch(config)#ap dot11 5ghz cleanair alarm air-quality threshold 50`	Configures the alarm for the threshold value for air-quality for all the 5-GHz devices. Add the **No** form of the command to disable the alarm.
Step 3	**ap dot11 5ghz cleanair alarm device**{**canopy** | **cont-tx** | **dect-like** | **inv** | **jammer** | **nonstd** | **radar** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile**} **Example:**	Configures the alarm for the 5-GHz devices. Add the **no** form of the command to disable the alarm. • **canopy**—Canopy devices. • **cont-tx**—Continuous Transmitter.

	Command or Action	Purpose
	`Switch(config)#ap dot11 5ghz cleanair alarm device`	• **dect-like**—Digital Enhanced Cordless Communication (DECT) like phone. • **fh**—802.11 frequency hopping devices. • **inv**—Devices using spectrally inverted WiFi signals. • **jammer**—Jammer. • **nonstd**—Devices using non-standard WiFi channels. • **radar**—Radars. • **report**—Interference device reporting. • **superag**—802.11 SuperAG devices. • **tdd-tx**—TDD Transmitter. • **video**—Video cameras. • **wimax-fixed**—WiMax Fixed. • **wimax-mobile**—WiMax Mobile.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for CleanAir, on page 1
Restrictions on CleanAir, on page 2
CleanAir FAQs, on page 26

Configuring Interference Reporting for 5-GHz devices

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 5ghz cleanair device** {**canopy** | **cont-tx** | **dect-like** | **inv** | **jammer** | **nonstd** |	Configures the 5-GHz interference devices to report to the switch. Add the **no** form of the command to disable interference device reporting.

	Command or Action	Purpose

	radar | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile}
	Example:
	`Switch(config)#ap dot11 5ghz cleanair device canopy`
	`Switch(config)#ap dot11 5ghz cleanair device cont-tx`
	`Switch(config)#ap dot11 5ghz cleanair device dect-like`
	`Switch(config)#ap dot11 5ghz cleanair device inv`
	`Switch(config)#ap dot11 5ghz cleanair device jammer`
	`Switch(config)#ap dot11 5ghz cleanair device nonstd`
	`Switch(config)#ap dot11 5ghz cleanair device radar`
	`Switch(config)#ap dot11 5ghz cleanair device report`
	`Switch(config)#ap dot11 5ghz cleanair device superag`
	`Switch(config)#ap dot11 5ghz cleanair device tdd-tx`
	`Switch(config)#ap dot11 5ghz cleanair device video`
	`Switch(config)#ap dot11 5ghz cleanair device wimax-fixed`
	`Switch(config)#ap dot11 5ghz cleanair device wimax-mobile`
		• **canopy**—Canopy devices
		• **cont-tx**—Continuous Transmitter
		• **dect-like**—Digital Enhanced Cordless Communication (DECT) like phone
		• **fh**—802.11 frequency hopping devices
		• **inv**—Devices using spectrally inverted WiFi signals
		• **jammer**—Jammer
		• **nonstd**—Devices using non-standard WiFi channels
		• **radar**—Radars
		• **report**—Interference device reporting
		• **superag**—802.11 SuperAG devices
		• **tdd-tx**—TDD Transmitter
		• **video**—Video cameras
		• **wimax-fixed**—WiMax Fixed
		• **wimax-mobile**—WiMax Mobile

Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for CleanAir, on page 1
Restrictions on CleanAir, on page 2
CleanAir FAQs, on page 26
Monitoring the Interference Devices (GUI), on page 24

Configuring EDRRM for CleanAir-Events

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event**
	Example:
	`Switch(config)#ap dot11 24ghz rrm channel cleanair-event`
	`Switch(config)#no ap dot11 24ghz rrm channel cleanair-event`
		Enables EDRRM cleanair-event. Add the **no** form of the command to disable EDRRM.

Step 3	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event** [**sensitivity** {**high** | **low** | **medium**}] **Example:** `Switch(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high`	Configures the EDRRM sensitivity of cleanair-event. • **High**—Specifies the most sensitivity to non Wi–Fi interference as indicated by the air quality (AQ) value. • **Low**—Specifies the least sensitivity to non Wi–Fi interference as indicated by the AQ value. • **Medium**—Specifies medium sensitivity to non Wi–Fi interference as indicated by the AQ value.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

EDRRM and AQR Update Mode, on page 7

Configuring Persistent Device Avoidance

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Switch# configure terminal`	
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel device** **Example:** `Switch(config)#ap dot11 24ghz rrm channel device`	Enables the persistent non Wi–Fi device avoidance in the 802.11 channel assignment. Add the **no** form of the command to disable the persistent device avoidance.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Cisco CleanAir using the Controller GUI

Configuring Cisco CleanAir on the Cisco Wireless LAN Controller (GUI)

Procedure

Step 1 Choose **Configuration > Wireless** > **802.11a/n/ac or 802.11b/g/n > CleanAir** to open the **802.11a (or 802.11b) > CleanAir** page.

Step 2 Select the **CleanAir** check box to enable Cisco CleanAir functionality on the 802.11a/n or 802.11b/g/n network, or unselect it to prevent the switch from detecting spectrum interference. By default, the Cisco CleanAir is disabled.

Step 3 Select the **Report Interferers** check box to enable the Cisco CleanAir system to report any detected sources of interference, or unselect it to prevent the switch from reporting interferers. The default value is selected.

Note Device Security alarms, Event Driven RRM, and the Persistence Device Avoidance algorithm do not work if Report Interferers are disabled.

Step 4 Select the **Persistent Device Propagation** check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables you to propagate information about persistent devices to the neighboring access points connected to the same switch. Persistent interferers are present at the location and interfere with the WLAN operations even if they are not detectable at all times.

Step 5 Ensure that any sources of interference that need to be detected and reported by the Cisco CleanAir system appear in the Interferences to Detect box and any that do not need to be detected appear in the Interferences to Ignore box. Use the **>** and **<** buttons to move interference sources between these two boxes. By default, all interference sources are detected. The sources of interference that you can choose depend on the type of radio, 802.11a/n/ac or 802.11b/g/n, and are as follows:

- **802.11 FH**—A 802.11 FH device
- **802.15.4**—A 802.15.4 or ZigBee device
- **Continuous Transmitter**—A continuous transmitter
- **Bluetooth Discovery**—A Bluetooth device

- **DECT-like Phone**—A digital enhanced cordless communication (DECT)-compatible phone
- **Microsoft**—A Microsoft device
- **SuperAG**—A 802.11a/g SuperAG device
- **Microwave Phone**—A microwave phone
- **Jammer**—A jamming device
- **Canopy**—A canopy bridge device
- **TDD Transmitter**—A time division duplex (TDD) transmitter device
- **Video Camera**—An analog video camera
- **WiFi Invalid Channel**—A WiFi invalid channel
- **WiFi Inverted**—A device using spectrally inverted Wi-Fi signals (I and Q signals of the RF signal are inverted)
- **WiMAX Fixed**—A WiMAX fixed device (802.11a/n/ac only)
- **WiMAX Mobile**—A WiMAX mobile device (802.11a/n/ac only)

Note Access points that are associated to the switch send interference reports only for the interferers that appear in the Interferences to Detect box. This functionality allows you to filter out interferers that you do not want as well as any that may be flooding the network and causing performance problems for the switch or Prime Infrastructure. Filtering allows the system to resume normal performance levels.

Step 6 Configure Cisco CleanAir alarms as follows:

a) Select the **Enable AQI (Air Quality Index) Trap** check box to enable the triggering of air quality alarms, or unselect the box to disable this feature. The default value is selected.

b) If you selected the **Enable AQI Trap** check box in *Step a*, enter a value between 1 and 100 (inclusive) in the AQI Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.

c) Enter the AQI threshold in the **AQI Alarm Threshold** text box. An alarm is generated when the air quality reaches a threshold value. The default is 35. The range is from 1 and 100.

d) Select the **Enable Interference For Security Alarm** check box to trigger interferer alarms when the switch detects specified device types, or unselect it to disable this feature. The default value is selected

e) Make sure that any sources of interference that need to trigger interferer alarms appear in the **Trap on These Types** box and any that do not need to trigger interferer alarms appear in the **Do Not Trap on These Types** box. Use the **>** and **<** buttons to move interference sources between these two boxes. By default, all interference sources trigger interferer alarms.

For example, if you want the switch to send an alarm when it detects a jamming device, select the **Enable Interference For Security Alarm** check box and move the jamming device to the **Trap on These Types** box.

Step 7 Click **Apply**.

Step 8 Trigger spectrum event-driven radio resource management (RRM) to run when a Cisco CleanAir-enabled access point detects a significant level of interference as follows:

a) Look at the **EDRRM** field to see the current status of spectrum event-driven RRM and, if enabled, the Sensitivity Threshold field to see the threshold level at which event-driven RRM is invoked.

b) If you want to change the current status of event-driven RRM or the sensitivity level, go to the **802.11a (or 802.11b) > RRM > Dynamic Channel Assignment (DCA)** page.

c) Select the **EDRRM** check box to trigger RRM to run when an access point detects a certain level of interference, or unselect it to disable this feature. The default value is selected.

d) If you selected the **EDRRM** check box in *Step c*, choose **Low**, **Medium**, **High** , or **Custom** from the Sensitivity Threshold drop-down list to specify the threshold at which you want RRM to be triggered. When the interference for the access point rises above the threshold level, RRM initiates a local dynamic channel assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. EDRRM prevents the access point from returning to the original channel for three hours after the event.

High—Represents an increased sensitivity to changes in the environment.

Custom—Allows you to set a threshold value in the Custom Sensitivity Threshold field. The default sensitivity is 35.

Low—Represents a decreased sensitivity to changes in the environment.

The EDRRM AQ threshold value for low sensitivity is 35, medium sensitivity is 50, and high sensitivity is 60.

e) Click **Apply**.

Step 9 Click **Save Configuration**.

Configuring Cisco CleanAir on an Access Point (GUI)

Procedure

Step 1 Choose **Configuration > Wireless** > **Access Points > Radios > 802.11a/n or 802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page.

Step 2 Select the check box adjacent to the desired access point and click **Configure**. The 802.11a/n/ac (or 802.11b/g/n) Radios page appears.

The **CleanAir Capable** field shows whether this access point can support CleanAir functionality. If it can, go to the next step to enable or disable CleanAir for this access point. If the access point cannot support CleanAir functionality, you cannot enable CleanAir for this access point.

Note By default, the Cisco CleanAir functionality is enabled on the radios.

Step 3 Enable Cisco CleanAir functionality for this access point by choosing **Enable** from the CleanAir Admin Status drop-down list. To disable CleanAir functionality for this access point, choose **Disable**. The default value is Enable. This setting overrides the global CleanAir configuration for this access point.

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Configuring Cisco Spectrum Expert

Configuring Spectrum Expert (GUI)

Before you begin

- Spectrum Expert (Windows XP laptop client) and access point should be pingable, otherwise; it will not work.
- Prior to establishing a connection between the Spectrum Expert console and the access point, make sure that IP address routing is properly configured and the network spectrum interface (NSI) ports are open in any intervening firewalls.
- The access point must be a TCP server listening on ports 37540 for 2.4 GHz and 37550 for 5 GHz frequencies. These ports must be opened for the spectrum expert application to connect to the access point using the NSI protocol.
- You can view the NSI key from the switch CLI by using the **show ap name** *ap_name* **config dot11** {**24ghz** | **5ghz**} command.

Procedure

Step 1 Ensure that Cisco CleanAir functionality is enabled for the access point that will be connected to the Spectrum Expert console.

Note The SE-Connect mode is set for the entire access point, not just a single radio. However, the Spectrum Expert console connects to a single radio at a time.

Step 2 Choose **Configuration** > **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 3 Click the name of the desired access point to open the All APs > Details page.

Step 4 Choose **SE-Connect** from the AP Mode drop-down list. This mode is available only for access points that are capable of supporting Cisco CleanAir functionality. For the SE-Connect mode to appear as an available option, the access point must have at least one spectrum-capable radio in the Enable state.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **OK** when prompted to reboot the access point.

Step 7 On the Windows PC, access the Cisco Software Center from this URL:

http://www.cisco.com/cisco/software/navigator.html

Step 8 Click **Product > Wireless > Cisco Spectrum Intelligence** > **Cisco Spectrum Expert** > **Cisco Spectrum Expert Wi-Fi**, and then download the Spectrum Expert 4.1.11 executable (*.exe) file.

Step 9 Run the Spectrum Expert application on the PC.

Step 10 When the Connect to Sensor dialog box appears, enter the IP address of the access point, choose the access point radio, and enter the 16-byte network spectrum interface (NSI) key to authenticate. The Spectrum Expert application opens a TCP/IP connection directly to the access point using the NSI protocol.

When an access point in SE-Connect mode joins a switch, it sends a Spectrum Capabilities notification message, and the switch responds with a Spectrum Configuration Request. The request contains the 16-byte random NSI key generated by the switch for NSI authentication. The switch generates one key per access point, which the access point stores until it is rebooted.

Note You can establish up to three Spectrum Expert console connections per access point radio.

Step 11 Verify that the Spectrum Expert console is connected to the access point by selecting the Slave Remote Sensor text box in the bottom right corner of the Spectrum Expert application. If the two devices are connected, the IP address of the access point appears in this text box.

Step 12 Use the Spectrum Expert application to view and analyze spectrum data from the access point.

Configuring Spectrum Expert (CLI)

Before you begin

- Spectrum Expert (Windows XP laptop client) and access point should be pingable, otherwise; it will not work.
- Prior to establishing a connection between the Spectrum Expert console and the access point, make sure that IP address routing is properly configured and the network spectrum interface (NSI) ports are open in any intervening firewalls.
- The access point must be a TCP server listening on ports 37540 for 2.4-GHz and 37550 for 5-GHz frequencies. These ports must be opened for the spectrum expert application to connect to the access point using the NSI protocol.
- You can view the NSI key from the switch CLI by using the **show ap name** *ap_name* **config dot11** {**24ghz** | **5ghz**} command.

Procedure

Step 1 To configure the access point for SE-Connect mode, enter this command:

ap name *ap_name* **mode se-connect**

Example:

```
Switch#ap name Cisco_AP3500 mode se-connect
```

Step 2 When prompted to reboot the access point, enter **Y**.

Step 3 To view the NSI key for the access point, enter this command:

show ap name *ap_name* **config dot11** {**24ghz** | **5ghz**}

Example:

```
Switch#show ap name Cisco_AP3500 config dot11 24ghz

<snippet>
CleanAir Management Information
    CleanAir Capable                          : Yes
    CleanAir Management Admin State           : Enabled
    CleanAir Management Operation State       : Up
```

```
    CleanAir NSI Key                              : 274F1F9B1A5206683FAF57D87BFFBC9B
    CleanAir Sensor State                         : Configured

<snippet>
```

What to do next

On the Windows PC, download Cisco Spectrum Expert:

- Access the Cisco Software Center from this URL: http://www.cisco.com/cisco/software/navigator.html
- Click **Product > Wireless > Cisco Spectrum Intelligence** > **Cisco Spectrum Expert** > **Cisco Spectrum Expert Wi-Fi**, and then download the Spectrum Expert 4.1.11 executable (*.exe) file.
- Run the Spectrum Expert application on the PC.
- When the Connect to Sensor dialog box appears, enter the IP address of the access point, choose the access point radio, and enter the 16-byte network spectrum interface (NSI) key to authenticate. The Spectrum Expert application opens a TCP/IP connection directly to the access point using the NSI protocol.

  When an access point in SE-Connect mode joins a switch, it sends a Spectrum Capabilities notification message, and the switch responds with a Spectrum Configuration Request. The request contains the 16-byte random NSI key generated by the switch for use in NSI authentication. The switch generates one key per access point, which the access point stores until it is rebooted.

  Note You can establish up to three Spectrum Expert console connections per access point radio.

- Verify that the Spectrum Expert console is connected to the access point by selecting the Slave Remote Sensor text box in the bottom right corner of the Spectrum Expert application. If the two devices are connected, the IP address of the access point appears in this text box.
- Use the Spectrum Expert application to view and analyze spectrum data from the access point.

Monitoring CleanAir Parameters

You can monitor CleanAir parameters using the following commands:

Table 2: Commands for Monitoring CleanAir

Commands	Description
show ap dot11 24ghz cleanair air-quality summary	Displays CleanAir Air Quality (AQ) data for 2.4-GHz band
show ap dot11 24ghz cleanair air-quality worst	Displays CleanAir Air Quality (AQ) worst data for 2.4-GHz band
show ap dot11 24ghz cleanair config	Displays CleanAir Configuration for 2.4-GHz band

Commands	Description
show ap dot11 24ghz cleanair device type all	Displays all CleanAir Interferers for 2.4-GHz band
show ap dot11 24ghz cleanair device type bt-discovery	Displays CleanAir Interferers of type BT Discovery for 2.4-GHz band
show ap dot11 24ghz cleanair device type bt-link	Displays CleanAir Interferers of type BT Link for 2.4-GHz band
show ap dot11 24ghz cleanair device type canopy	Displays CleanAir Interferers of type Canopy for 2.4-GHz band
show ap dot11 24ghz cleanair device type cont-tx	Displays CleanAir Interferers of type Continuous transmitter for 2.4-GHz band
show ap dot11 24ghz cleanair device type dect-like	Displays CleanAir Interferers of type DECT Like for 2.4-GHz band
show ap dot11 24ghz cleanair device type fh	Displays CleanAir Interferers of type 802.11FH for 2.4-GHz band
show ap dot11 24ghz cleanair device type inv	Displays CleanAir Interferers of type WiFi Inverted for 2.4-GHz band
show ap dot11 24ghz cleanair device type jammer	Displays CleanAir Interferers of type Jammer for 2.4-GHz band
show ap dot11 24ghz cleanair device type mw-oven	Displays CleanAir Interferers of type MW Oven for 2.4-GHz band
show ap dot11 24ghz cleanair device type nonstd	Displays CleanAir Interferers of type WiFi Inv. Ch for 2.4-GHz band
show ap dot11 24ghz cleanair device type persistent	Displays CleanAir Interferers of type Persistent for 2.4-GHz band
show ap dot11 24ghz cleanair device type superag	Displays CleanAir Interferers of type SuperAG for 2.4-GHz band
show ap dot11 24ghz cleanair device type tdd-tx	Displays CleanAir Interferers of type TDD Transmit for 2.4-GHz band
show ap dot11 24ghz cleanair device type video	Displays CleanAir Interferers of type Video Camera for 2.4-GHz band
show ap dot11 24ghz cleanair device type wimax-fixed	Displays CleanAir Interferers of type WiMax Fixed for 2.4-GHz band
show ap dot11 24ghz cleanair device type wimax-mobile	Displays CleanAir Interferers of type WiMax Mobile for 2.4-GHz band
show ap dot11 24ghz cleanair device type xbox	Displays CleanAir Interferers of type Xbox for 2.4-GHz band

Commands	Description
show ap dot11 24ghz cleanair device type zigbee	Displays CleanAir Interferers of type zigbee for 2.4-GHz band
show ap dot11 5ghz cleanair air-quality summary	Displays CleanAir Air Quality (AQ) data for 5-GHz band
show ap dot11 5ghz cleanair air-quality worst	Displays CleanAir Air Quality (AQ) worst data for 5-GHz band
show ap dot11 5ghz cleanair config	Displays CleanAir Configuration for 5-GHz band
show ap dot11 5ghz cleanair device type all	Displays all CleanAir Interferers for 5-GHz band
show ap dot11 5ghz cleanair device type canopy	Displays CleanAir Interferers of type Canopy for 5-GHz band
show ap dot11 5ghz cleanair device type cont-tx	Displays CleanAir Interferers of type Continuous TX for 5-GHz band
show ap dot11 5ghz cleanair device type dect-like	Displays CleanAir Interferers of type DECT Like for 5-GHz band
show ap dot11 5ghz cleanair device type inv	Displays CleanAir Interferers of type WiFi Inverted for 5-GHz band
show ap dot11 5ghz cleanair device type jammer	Displays CleanAir Interferers of type Jammer for 5-GHz band
show ap dot11 5ghz cleanair device type nonstd	Displays CleanAir Interferers of type WiFi Inv. Ch for 5-GHz band
show ap dot11 5ghz cleanair device type persistent	Displays CleanAir Interferers of type Persistent for 5-GHz band
show ap dot11 5ghz cleanair device type superag	Displays CleanAir Interferers of type SuperAG for 5-GHz band
show ap dot11 5ghz cleanair device type tdd-tx	Displays CleanAir Interferers of type TDD Transmit for 5-GHz band
show ap dot11 5ghz cleanair device type video	Displays CleanAir Interferers of type Video Camera for 5-GHz band
show ap dot11 5ghz cleanair device type wimax-fixed	Displays CleanAir Interferers of type WiMax Fixed for 5-GHz band
show ap dot11 5ghz cleanair device type wimax-mobile	Displays CleanAir Interferers of type WiMax Mobile for 5-GHz band

You can also check the CleanAir status of the access points using the switch GUI:

Procedure

Choose **Monitor** > **Wireless** > **Access Points** > **802.11 a/n/ac**or **802.11 b/g/n**.

The **Radios** page is displayed showing a list of access points that are associated with the switch. You can see the CleanAir Admin and CleanAir Status.

The Cisco CleanAir status is one of the following:

- **UP**—The spectrum sensor for the access point radio is currently operational (error code 0).
- **DOWN**—The spectrum sensor for the access point radio is currently not operational because an error has occurred. The most likely reason for the error is that the access point radio is disabled (error code 8). To correct this error, enable the radio.
- **ERROR**—The spectrum sensor for the access point radio has crashed (error code 128), making CleanAir monitoring nonoperational for this radio. If this error occurs, reboot the access point. If the error continues to appear, you might want to disable Cisco CleanAir functionality on the radio.
- **N/A**—This access point radio is not capable of supporting Cisco CleanAir functionality.

Monitoring the Interference Devices

When a CleanAir-enabled access point detects interference devices, detections of the same device from multiple sensors are merged together to create clusters. Each cluster is given a unique ID. Some devices conserve power by limiting the transmit time until actually needed which results in the spectrum sensor to temporarily stop detecting the device. This device is then correctly marked as down. A down device is correctly removed from the spectrum database. In cases when all the interferer detections for a specific devices are reported, the cluster ID is kept alive for an extended period of time to prevent possible device detection bouncing. If the same device is detected again, it is merged with the original cluster ID and the device detection history is preserved.

For example, some bluetooth headsets operate on battery power. These devices employ methods to reduce power consumption, such as turning off the transmitter when not actually needed. Such devices can appear to come and go from the classification. To manage these devices, CleanAir keeps the cluster IDs longer and they are remerged into a single record upon detection. This process smoothens the user records and accurately represents the device history.

Monitoring the Interference Devices (GUI)

Before you begin

You can configure Cisco CleanAir only on CleanAir-enabled access points.

Procedure

Step 1 Choose **Monitor > Interferers > Cisco CleanAir > 802.11a/n or 802.11b/g/n > Interference Devices** to open the Cisco APs > Interference Devices page.

This page shows the following information:

- **AP Name**—The name of the access point where the interference device is detected.

- **Interferer Type**—Type of the interferer.
- **Affected Channel**—Channel that the device affects.
- **Severity**—Severity index of the interfering device.
- **Duty Cycle (%)**—Proportion of time during which the interfering device was active.
- **RSSI**—Receive signal strength indicator (RSSI) of the access point.
- **DevID**—Device identification number that uniquely identified the interfering device.
- **ClusterID**—Cluster identification number that uniquely identifies the type of the devices.

Step 2 Click the **Filter** icon or choose the **Quick Filter** option from the Show drop-down list to display the information about interference devices based on a particular criteria.

Related Topics

Configuring Interference Reporting for 2.4-GHz Devices, on page 10
Configuring Interference Reporting for 5-GHz devices, on page 13

Monitoring the Worst Air Quality of Radio Bands (GUI)

Procedure

Choose **Monitor** > **Cisco CleanAir** > **Worst Air-Quality** to open the Air Quality Report page.

This page shows the air quality of both the 802.11a/n/ac and 802.11b/g/n radio bands. This page displays the following information:

- **AP Name**—Name of the access point that reported the worst air quality for the 802.11 radio band.
- **Channel Number**—Radio channel with the worst reported air quality.
- **Minimum Air Quality Index**—Minimum air quality for this radio channel. The range is from 1 to 100. An air quality index (AQI) value of 100 is the best, and 1 is the worst.
- **Average Air Quality Index**—Average air quality for this radio channel. The range is from 1 to 100. An air quality index (AQI) value of 100 is the best, and 1 is the worst.
- **Interference Device Count**—Number of interferers detected by the radios on the 802.11 radio band.

Configuration Examples for Configuring CleanAir

Enabling CleanAir on 2.4-GHz Band and an Access Point: Example

This example shows how to enable CleanAir on the 2.4-GHz band and an access point operating in the channel:

```
Switch#configure terminal
Switch(config)#ap dot11 24ghz cleanair
Switch(config)#exit
Switch#ap name TAP1 dot11 24ghz cleanair
Switch#end
```

Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices: Example

This example shows how to configure a CleanAir Alarm for 2.4-GHz Air-Quality threshold of 50 dBm and an Xbox device:

```
Switch#configure terminal
Switch(config)#ap dot11 24ghz cleanair alarm air-quality threshold 50
Switch(config)#ap dot11 24ghz cleanair alarm device xbox
Switch(config)#end
```

Configuring Interference Reporting for 5-GHz Devices: Example

This example shows how to configure interference reporting for 5-GHz devices:

```
Switch#configure terminal
Switch(config)#ap dot11 5ghz cleanair alarm device xbox
Switch(config)#end
```

Configuring EDRRM for CleanAir-Events: Example

This example shows how to enable an EDRRM cleanair-event in the 2.4-GHz band and configure high sensitivity to non Wi–Fi interference:

```
Switch#configure terminal
Switch(config)#ap dot11 24ghz rrm channel cleanair-event
Switch(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high
Switch(config)#end
```

Configuring Persistent Device Avoidance: Example

This example shows how to enable persistent non Wi–Fi device avoidance in the 2.4-GHz band:

```
Switch#configure terminal
Switch(config)#ap dot11 24ghz rrm channel device
Switch(config)#end
```

Configuring an Access Point for SE-Connect Mode: Example

This example shows how to configure an access point in the SE-Connect mode:

```
Switch#ap name Cisco_AP3500 mode se-connect
```

CleanAir FAQs

Q. How do I check if my MC is up?

A. To check if the MC is up, use the command: **show wireless mobility summary**.

This example shows how to display the mobility summary:

```
Switch#show wireless mobility summary

Mobility Controller Summary:
Mobility Role                                 : Mobility Controller
```

```
Mobility Protocol Port                          : 16666
Mobility Group Name                             : MG-AK
Mobility Oracle                                 : Disabled
Mobility Oracle IP Address                      : 0.0.0.0
DTLS Mode                                       : Enabled
Mobility Domain ID for 802.11r                  : 0x39b2
Mobility Keepalive Interval                     : 10
Mobility Keepalive Count                        : 3
Mobility Control Message DSCP Value             : 48
Mobility Domain Member Count                    : 2
Link Status is Control Link Status : Data Link Status
Controllers configured in the Mobility Domain:
IP              Public IP       Group Name       Multicast IP     Link Status
------------------------------------------------------------------------------
9.6.136.10      -               MG-AK            0.0.0.0          UP   : UP
```

Q. Multiple access points detect the same interference device, however, the switch shows them as separate clusters or different suspected devices clustered together. Why does this happen?

A. Access points must be RF neighbors for the switch to consider the merging of devices that are detected by these access points. The access point takes time to establish neighbor relationships. A few minutes after the switch reboots or a change in the RF group and similar events, clustering will not be very accurate.

Q. Can I merge two monitor mode access points using a switch?

A. No, you cannot merge two monitor mode access points using a switch. You can merge the monitor mode access points only using MSE.

Q. How do I view neighbor access points?

A. To view neighbor access points, use the command: **show ap** *ap_name* **auto-rf dot11** {**24ghz** | **5ghz**}

This example shows how to display the neighbor access points:

```
Switch#show ap name AS-5508-5-AP3 auto-rf dot11 24ghz

<snippet>
Nearby APs
  AP 0C85.259E.C350 slot 0                          :  -12 dBm on   1 (10.10.0.5)
  AP 0C85.25AB.CCA0 slot 0                          :  -24 dBm on   6 (10.10.0.5)
  AP 0C85.25C7.B7A0 slot 0                          :  -26 dBm on  11 (10.10.0.5)
  AP 0C85.25DE.2C10 slot 0                          :  -24 dBm on   6 (10.10.0.5)
  AP 0C85.25DE.C8E0 slot 0                          :  -14 dBm on  11 (10.10.0.5)
  AP 0C85.25DF.3280 slot 0                          :  -31 dBm on   6 (10.10.0.5)
  AP 0CD9.96BA.5600 slot 0                          :  -44 dBm on   6 (10.0.0.2)
  AP 24B6.5734.C570 slot 0                          :  -48 dBm on  11 (10.0.0.2)
<snippet>
```

Q. What are the debug commands available for CleanAir?

A. The debug commands for CleanAir are:

debug cleanair {**all** | **error** | **event** | **internal-event** | **nmsp** | **packet**}

debug rrm {**all** | **channel** | **detail** | **error** | **group** | **ha** | **manager** | **message** | **packet** | **power** | **prealarm** | **profile** | **radar** | **rf-change** | **scale** | **spectrum**}

Q. Why are CleanAir Alarms not generated for interferer devices?

A. Verify that the access points are CleanAir-capable and CleanAir is enabled both on the access point and the switch.

Q. Can the Cisco Catalyst 3850 Series Switches function as a Mobility Agent (MA)?

A. Yes, the Cisco Catalyst 3850 Series Switches can function as an MA.

Q. Are CleanAir configurations available on the MA?

A. From Release 3.3 SE, CleanAir configurations are available on the MA. You can use the following two CleanAir commands on the MA:

- **show ap dot11 5ghz cleanair config**
- **show ap dot11 24ghz cleanair config**

Related Topics

Enabling CleanAir for 2.4-GHz Band, on page 8
Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices, on page 9
Configuring Interference Reporting for 2.4-GHz Devices, on page 10
Enabling CleanAir for 5-GHz Band, on page 12
Configuring a CleanAir Alarm for 5-GHz Air-Quality and Devices, on page 12
Configuring Interference Reporting for 5-GHz devices, on page 13

Additional References

Related Documents

Related Topic	Document Title
CleanAir commands and their details	*CleanAir Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)CleanAir Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
High Availability configurations	*High Availability Configuration Guide, Cisco IOS XE Release 3SE (Cisco 5700 Series Wireless Controllers)*
High Availability commands and their details	*High Availability Command Reference, Cisco IOS XE Release 3SE (Cisco 5700 Series Wireless Controllers)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

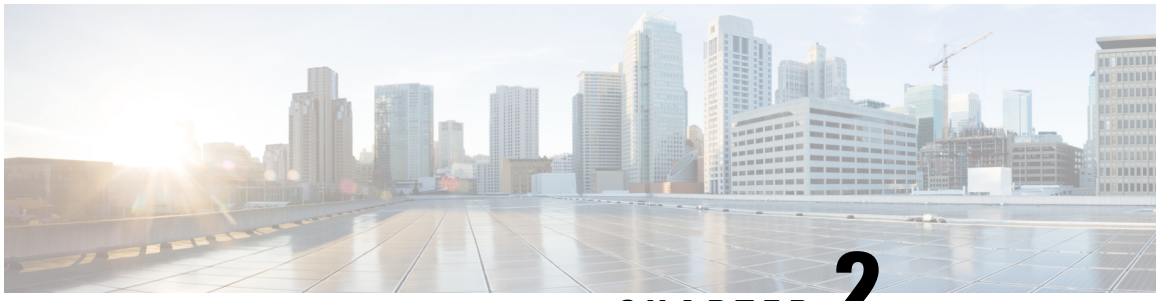
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

PART II

High Availability



CHAPTER 2

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information about High Availability

The high availability feature is enabled by default when the switches are connected using the stack cable and the technology is enabled. You cannot disable it; however, you can initiate a manual graceful-switchover using the command line interface to use the high availability feature enabled in the switch.

In Cisco Wireless LAN Controllers, high availability is achieved with redundancy.

In Cisco Wireless LAN Controllers, redundancy is achieved in two ways— n+1 and AP SSO redundancy.

Keepalive messages are sent and received between the active and standby controllers.

- If the standby controller does not respond, a new standby controller is elected.
- If the active controller does not respond, the standby controller becomes the active controller.

In addition, hello messages are sent and received by all stack members.

- If a stack member does not respond, that member is removed from the stack.
- If the standby controller does not respond, a new standby controller is elected.

- If the active controller does not respond, the standby controller becomes the active controller.

Information About Redundancy

In case of n+1 redundancy, access points are configured with primary, secondary, and tertiary controllers. When the primary controller fails, depending upon the number of access points managed by a controller, the access point fails over to the secondary controller. In case of AP SSO redundancy, once the primary controller is unavailable, the access points re-discovers the controller and reestablishes the CAPWAP tunnel with the secondary controller. However, all clients must disconnect and a re-authentication is performed to rejoin the controller.

You can configure primary, secondary, and tertiary controllers for a selected access point and a selected controller.

In an ideal high availability deployment, you can have access points connected to primary and secondary controllers and one controller can remain with out connection to any access points. This way the controller that does not have any access points can take over when a failure occurs and resume services of active controller.

Configuring Redundancy in Access Points

You must use the commands explained in this section to configure primary, secondary, or tertiary controllers for a selected access point.

Before you begin

Procedure

	Command or Action	Purpose
Step 1	conf t **Example:** `Controller # conf t`	Configures the terminal
Step 2	ap capwap backup primary **Example:** `Controller # ap capwap backup primary WLAN-Controller-A`	Configures the primary controller for the selected access point.
Step 3	**ap capwap backup secondary** **Example:** `Controller # ap capwap backup secondary WLAN-Controller-B`	Configures the secondary controller for the selected access point.
Step 4	ap capwap backup tertiary **Example:** `Controller # ap capwap backup tertiary WLAN-Controller-C`	Configures the tertiary controller for the selected access point.

What to do next

Once you complete configuration of the primary, secondary, and tertiary controllers for a selected access point, you must verify the configuration using the **show ap name** *AP-NAME* command. For more details on, **show ap name** *AP-NAME* command, see the Lightweight Access Point Configuration Guide for Cisco Wireless LAN Controller.

-

Configuring Heartbeat Messages

Hearbeat messages enable you to reduce the controller failure detection time. When a failure occurs, a switchover from active to hot standby happens after the controller waits for the heartbeat timer. If the controller does not function within the heartbeat time, then the standby takes over as then active controller. Ideally the access point generates three heartbeat messages within the time out value specified, and when the controller does not respond within the timeout value, the standby controller takes over as active. You can specify the timeout value depending on your network. Ideally the timer value is not a higher value as some chaos will occur while performing a switchover. This section explains on how to configure heartbeat interval between the controller and the access points using a timeout value to reduce the controller failure detection time.

Before you begin

Procedure

	Command or Action	Purpose
Step 1	conf t **Example:** `controller # conf t`	Configures the terminal.
Step 2	ap capwap timers heartbeat-timeout **Example:** `controller #  ap capwap timers heartbeat-timeout`	Configures the heartbeat interval between the controller and access points. The timeout value ranges from 1 to 30.

Information about Access Point Stateful Switch Over

An Access Point Stateful Switch Over (AP SSO) implies that all the access point sessions are switched over state-fully and the user session information is maintained during a switchover, and access points continue to operate in network with no loss of sessions, providing improved network availability. The active switch in the stack is equipped to perform all network functions, including IP functions and routing information exchange. The switch supports 1000 access points and 12000 clients.

However, all the clients are de-authenticated and need to be re-associated with the new active switch except for the locally switched clients in FlexConnect mode when a switchover occurs.

Once a redundancy pair is formed while in a stack, high availability is enabled, which includes that access points continue to remain connected during an active-to-standby switchover.

Note You can not disable AP SSO while in a switch stack once the switches form a redundant pair.

Note After switchover new standby gets reloaded during stack formation, this is due to bulk sync failure. This is seen after reload, 2nd attempt to form stack successfully. This happens when you execute the command *exception dump device second flash* which is used to enable, dump crashfile on flash when crashinfo directory is full. When crash occurs and if there is no space left in crashinfo, it proceeds to store the fullcore or crash files into flash.

Initiating Graceful Switchover

To perform a manual switchover and to use the high availability feature enabled in the switch, execute the **redundancy force-switchover** command. This command initiates a graceful switchover from the active to the standby switch.

```
Switch# redundancy force-switchover
System configuration has been modified. Save ? [yes/no] : yes
Building configuration …
Preparing for switchover …
Compressed configuration from 14977 bytes to 6592 bytes[OK]This will reload the active unit
 and force switchover to standby[confirm] : y
```

Configuring EtherChannels for High Availability

The LAG, or an EtherChannel, bundles all the existing ports in both the standby and active units into a single logical port to provide an aggregate bandwidth of 60 Gbps. The creation of an EtherChannel enables protection against failures. The EtherChannels or LAGs created are used for link redundancy to ensure high availability of access points.

For more details on configuring EtherChannel, and Etherchannel modes, see the Layer 2 (Link Aggregation) Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)

Procedure

Step 1 Connect two switches that are in powered down state using the stack cable.

Step 2 Power up and perform a boot on both switches simultaneously or power and boot one switch.

The switches boot up successfully, and form a high availability pair.

Step 3 Configure EtherChannel or LAG on the units.

Step 4 Use the **show etherchannel summary** command to view the status of the configured EtherChannel.

On successful configuration, all the specified ports will be bundled in a single channel and listed in the command output of **show etherchannel summary**.

Step 5 Execute the **show ap uptime** command to verify the connected access points.

Configuring LACP

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**interface port-channel** *number* **Example:** `Switch(config)# interface Port-channel Po2`	Enters port-channel interface configuration mode.
Step 3	**lacp max-bundle** *number* **Example:** `Switch(config-if)# lacp max-bundle 6`	Defines the maximum number of active bundled LACP ports allowed in a port channel. The value ranges from 1 to 8.
Step 4	**lacp port-priority** *number* **Example:** `Switch(config-if)# lacp port-priority 4`	Specifies port priority to be configured on the port using LACP. The value ranges from 0 to 65535.
Step 5	**switchport backup interface** *po2* **Example:** `Switch(config-if)# switchport backup interface Po2`	Specifies an interface as the backup interface.
Step 6	**end**	Exits the interface and configuration mode.
Step 7	**show etherchannel summary** **Example:** `Switch# show etherchannel summary`	Displays a summary of EtherChannel properties.
Step 8	**show interfaces switchport backup** **Example:** `Switch# show interfaces switchport backup`	Displays summary of backup EtherChannel properties.

Troubleshooting High Availability

Access the Standby Console

You can only access the console of the active switch in a stack. To access the standby switch, use the following commands.

Before you begin

Use this functionality only under supervision of Cisco Support.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**service internal** **Example:** `Switch(config)# service internal`	Enables Cisco IOS debug commands.
Step 3	**redundancy** **Example:** `Switch(config)# redundancy`	Enters redundancy configuration mode.
Step 4	**main-cpu** **Example:** `Switch(config)# main-cpu`	Enters the redundancy main configuration submode.
Step 5	**standby console enable** **Example:** `Switch(config)# standby console enable`	Enables the standby console.
Step 6	**exit** **Example:** `Switch(config)# exit`	Exits the configuration mode.

Before a Switchover

A switchover happens when the active switch fails; however, while performing a manual switchover, you can execute these commands to initiate a successful switchover:

Procedure

	Command or Action	Purpose
Step 1	**show redundancy states** **Example:** `Switch# show redundancy states`	Displays the high availability role of the active and standby switches.
Step 2	**show switch detail** **Example:** `Switch# show switch detail`	Display physical property of the stack. Verify if the physical states of the stacks are "Ready" or "Port".
Step 3	**show platform ses states** **Example:** `Switch# show platform ses states`	Displays the sequences of the stack manager.
Step 4	**show ap summary** **Example:** `Switch# show ap summary`	Displays all the access points in the active and standby switches.
Step 5	**show capwap detail** **Example:** `Switch# show capwap detail`	Displays the details of the CAPWAP tunnel in the active and standby switches.
Step 6	**show dtls database-brief** **Example:** `Switch# show dtls database-brief`	Displays DTLS details in the active and standby switches.
Step 7	**show power inline** **Example:** `Switch# show power inline`	Displays the power on Ethernet power state. **Note** When a failover occurs, the standby controller must be in a standby-hot state and the redundant port in a terminal state in SSO for successful switchover to occur.

After a Switchover

This section defines the steps that you must perform to ensure that successful switchover from the active to standby switch is performed. On successful switchover of the standby switch as active, all access points connected to the active need to re-join the standby (then active) switch.

Procedure

	Command or Action	Purpose
Step 1	**show ap uptime** **Example:**	Verify if the uptime of the access point after the switchover is large enough.

	Command or Action	Purpose
	`Switch# show ap uptime`	
Step 2	**show wireless summary** **Example:** `Switch# show wireless summary`	Display the clients connected in the active switch.
Step 3	**show wcdb database all** **Example:** `Switch# show wcdb database all`	Display if the client has reached the uptime.
Step 4	**show power inline** **Example:** `Switch# show power inline`	Display the power over Ethernet power state.

Viewing Redundancy Switchover History (GUI)

Procedure

Step 1 Click **Monitor > Controller > Redundancy** > **States.**

The Redundancy States page is displayed. The values for the following parameters are displayed in the page:

Parameter	Description
Index	Displays the index number of the of the redundant unit.
Previous Active	Displays the Switches that was active before.
Current Active	Displays the Switches that is currently active.
Switch Over Time	Displays the system time when the switchover occurs.
Switch Over Reason	Displays the cause of the switchover.

Step 2 Click **Apply**.

Viewing Switchover States (GUI)

Procedure

Step 1 Click **Monitor > Controller > Redundancy** > **States.**

The Redundancy States page is displayed. The values for the following parameters are displayed in the page:

Parameter	Description
My State	Shows the state of the active CPU Switch module. Values are as follows: • Active • Standby HOT • Disable
Peer State	Displays the state of the peer (or standby) CPU Switch module. Values are as follows: • Standby HOT • Disable
Mode	Displays the current state of the redundancy peer. Values are as follows: • Simplex— Single CPU switch module • Duplex— Two CPU switch modules
Unit ID	Displays the unit ID of the CPU switch module.
Redundancy Mode (Operational)	Displays the current operational redundancy mode supported on the unit.
Redundancy Mode (Configured)	Displays the current configured redundancy mode supported on the unit.
Redundancy State	Displays the current functioning redundancy state of the unit. Values are as follows: • SSP • Not Redundant
Manual SWACT	Displays whether manual switchovers have been enabled without the force option.
Communications	Displays whether communications are up or down between the two CPU Switch modules.
Client Count	Displays the number of redundancy subsystems that are registered as RF clients.
Client Notification TMR	Displays, in milliseconds, the time that an internal RF timer has for notifying RF client subsystems.
Keep Alive TMR	Displays, in milliseconds, the time interval the RF manager has for sending keep-alive messages to its peer on the standby CPU switch module.
Keep Alive Count	Displays the number of keep-alive messages sent without receiving a response from the standby CPU Switch module.
Keep Alive Threshold	Displays the threshold for declaring that interprocessor communications are down when keep-alive messages have been enabled (which is the default).
RF Debug Mask	Displays an internal mask used by the RF to keep track of which debug modes are on.

Step 2 Click **Apply**.

Monitoring the Switch Stack

Table 3: Commands for Displaying Stack Information

Command	Description
show switch	Displays summary information about the stack, including the status of provisioned switches and switches in version-mismatch mode.
show switch *stack-member-number*	Displays information about a specific member.
show switch detail	Displays detailed information about the stack.
show switch neighbors	Displays the stack neighbors.
show switch stack-ports [**summary**]	Displays port information for the stack. Use the **summary** keyword to display the stack cable length, the stack link status, and the loopback status.
show redundancy	Displays the redundant system and the current processor information. The redundant system information includes the system uptime, standby failures, switchover reason, hardware, configured and operating redundancy mode. The current processor information displayed includes the active location, the software state, the uptime in the current state and so on.
show redundancy state	Displays all the redundancy states of the active and standby switches.

LACP Configuration: Example

This example shows how to configure LACP and to verify creation of the LACP bundle and the status:

```
Switch(config)# !
interface TenGigabitEthernet1/0/1
 switchport mode trunk
 channel-group 1 mode active
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/2
 switchport mode trunk
 channel-group 1 mode active
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/3
 switchport mode trunk
 channel-group 1 mode active
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/4
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
```

```
!
interface TenGigabitEthernet1/0/5
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/6
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/1
 switchport mode trunk
 channel-group 1 mode active
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/2
 switchport mode trunk
 channel-group 1 mode active
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/3
 switchport mode trunk
 channel-group 1 mode active
 lacp port-priority 10
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/4
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/5
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/6
 switchport mode trunk
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface Vlan1
 no ip address
 ip igmp version 1
 shutdown
!

Switch#  show etherchannel summary

  Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
```

```
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Te1/0/1(P)  Te1/0/2(P)  Te1/0/3(P)
                                 Te1/0/4(H)  Te1/0/5(H)  Te1/0/6(H)
                                 Te2/0/1(P)  Te2/0/2(P)  Te2/0/3(P)
                                 Te2/0/4(H)  Te2/0/5(H)  Te2/0/6(H)
```

This example shows the switch backup interface pairs:

```
Switch# show interfaces switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
Port-channel1             Port-channel2             Active Standby/Backup Up
```

This example shows the summary of the EtherChannel configured in the switch:

```
Switch# show ethernet summary

Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Te1/0/1(P)  Te1/0/2(P)  Te1/0/3(P)
                                 Te1/0/4(P)  Te1/0/5(P)  Te1/0/6(P)
2      Po2(SU)         LACP      Te2/0/1(P)  Te2/0/2(P)  Te2/0/3(P)
                                 Te2/0/4(P)  Te2/0/5(P)  Te2/0/6(P)
```

Flex Link Configuration: Example

This example shows how to configure flex link and to verify creation and the status of the created link:

```
Switch(config)# !
interface Port-channel1
 description Ports 1-6 connected to NW-55-SW
 switchport mode trunk
 switchport backup interface Po2
 switchport backup interface Po2 preemption mode forced
 switchport backup interface Po2 preemption delay 1
 ip dhcp snooping trust
!
interface Port-channel2
 description Ports 7-12connected to NW-55-SW
 switchport mode trunk
```

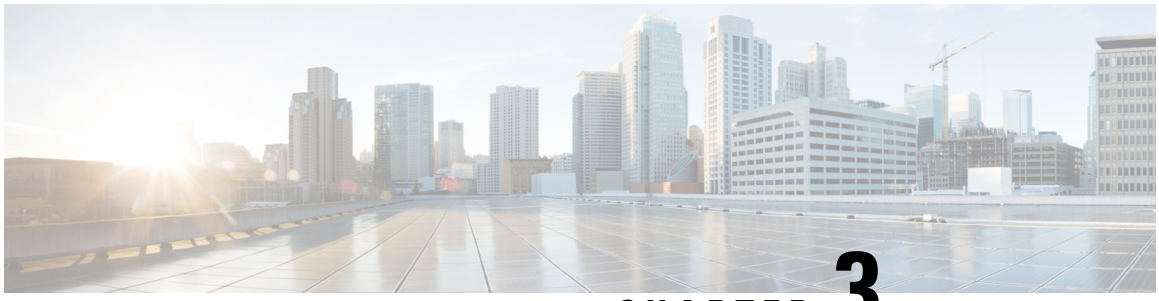
```
 ip dhcp snooping trust
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 no ip address
 negotiation auto
!
interface TenGigabitEthernet1/0/1
 switchport mode trunk
 channel-group 1 mode on
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/2
 switchport mode trunk
 channel-group 1 mode on
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/3
 switchport mode trunk
 channel-group 1 mode on
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/4
 switchport mode trunk
 channel-group 1 mode on
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/5
 switchport mode trunk
 channel-group 1 mode on
 ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/6
 switchport mode trunk
 channel-group 1 mode on
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/1
 switchport mode trunk
 channel-group 2 mode on
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/2
 switchport mode trunk
 channel-group 2 mode on
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/3
 switchport mode trunk
 channel-group 2 mode on
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/4
 switchport mode trunk
 channel-group 2 mode on
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/5
 switchport mode trunk
 channel-group 2 mode on
 ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/6
 switchport mode trunk
```

```
 channel-group 2 mode on
 ip dhcp snooping trust
!
interface Vlan1
 no ip address
```

```
Switch#  show etherchannel summary

Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)          -        Te1/0/1(P)  Te1/0/2(P)  Te1/0/3(P)
                                 Te1/0/4(P)  Te1/0/5(P)  Te1/0/6(P)
2      Po2(SU)          -        Te2/0/1(P)  Te2/0/2(P)  Te2/0/3(D)
                                 Te2/0/4(P)  Te2/0/5(P)  Te2/0/6(P)
```

PART III

IPv6



CHAPTER 3

Configuring IPv6 Client IP Address Learning

Prerequisites for IPv6 Client Address Learning

Before configuring IPv6 client address learning, configure the wireless clients to support IPv6.

Related Topics

Configuring RA Guard Policy, on page 55

Restrictions for IPv6 Client Address Learning

There are no specific requirements for IPv6 client address learning.

Information About IPv6 Client Address Learning

Client Address Learning is configured on switch to learn the wireless client's IPv4 and IPv6 address and clients transition state maintained by the switch on an association, re-association, de-authentication and timeout.

There are three ways for IPv6 client to acquire IPv6 addresses:

- Stateless Address Auto-Configuration (SLACC)
- Stateful DHCPv6
- Static Configuration

For all of these methods, the IPv6 client always sends neighbor solicitation DAD (Duplicate Address Detection) request to ensure there is no duplicate IP address on the network. The switch snoops the client's NDP and DHCPv6 packets to learn about its client IP addresses.

SLAAC Address Assignment

The most common method for IPv6 client address assignment is Stateless Address Auto-Configuration (SLAAC). SLAAC provides simple plug-and-play connectivity where clients self-assign an address based on the IPv6 prefix. This process is achieved

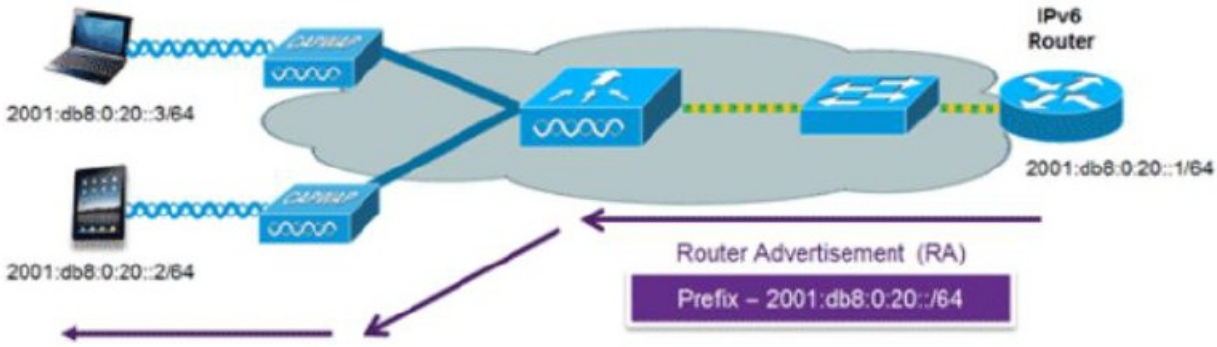
Stateless Address Auto-Configuration (SLAAC) is configured as follows:

- Host sends a router solicitation message.
- Hosts waits for a Router Advertisement message.
- Hosts take the first 64 bits of the IPv6 prefix from the Router Advertisement message and combines it with the 64 bit EUI-64 address (in the case of ethernet, this is created from the MAC Address) to create a global unicast message. The host also uses the source IP address, in the IP header, of the Router Advertisement message, as its default gateway.
- Duplicate Address Detection is performed by IPv6 clients in order to ensure that random addresses that are picked do not collide with other clients.
- The choice of algorithm is up to the client and is often configurable.

The last 64 bits of the IP v6 address can be learned based on the following 2 algorithms:

- EUI-64 which is based on the MAC address of the interface, or
- Private addresses that are randomly generated.

Figure 2: SLAAC Address Assignment



The following Cisco IOS configuration commands from a Cisco-capable IPv6 router are used to enable SLAAC addressing and router advertisements:

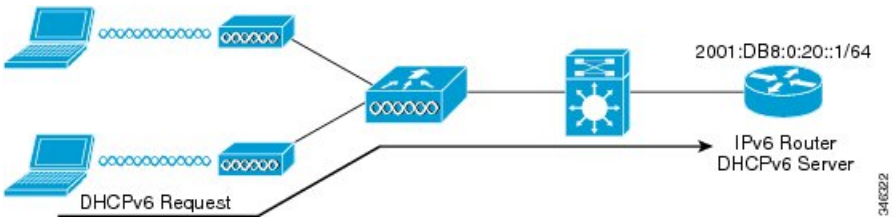
```
ipv6 unicast-routing
interface Vlan20
description IPv6-SLAAC
ip address 192.168.20.1 255.255.255.0
ipv6 address FE80:DB8:0:20::1 linklocal
ipv6 address 2001:DB8:0:20::1/64
ipv6 enable
end
```

Related Topics

Configuring IPv6 Snooping, on page 58
Configuring DHCP Pool , on page 62
Configuring Stateless Auto Address Configuration Without DHCP (CLI), on page 63
Configuring Stateless Auto Address Configuration With DHCP , on page 65
Configuring Stateful DHCP Locally, on page 66
Configuring Stateful DHCP Externally, on page 68

Stateful DHCPv6 Address Assignment

Figure 3: Stateful DHCPv6 Address Assignment



The use of DHCPv6 is not required for IPv6 client connectivity if SLAAC is already deployed. There are two modes of operation for DHCPv6 called Stateless and Stateful.

The DHCPv6 Stateless mode is used to provide clients with additional network information that is not available in the router advertisement, but not an IPv6 address as this is already provided by SLAAC. This information can include the DNS domain name, DNS server(s), and other DHCP vendor-specific options. This interface configuration is for a Cisco IOS IPv6 router implementing stateless DHCPv6 with SLAAC enabled:

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateless
ip address 192.168.20.1 255.255.255.0
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPOOL
ipv6 address 2001:DB8:0:20::1/64
end
```

The DHCPv6 Stateful option, also known as managed mode, operates similarly to DHCPv4 in that it assigns unique addresses to each client instead of the client generating the last 64 bits of the address as in SLAAC. This interface configuration is for a Cisco IOS IPv6 router implementing stateful DHCPv6 on a local Switch:

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateful
ip address 192.168.20.1 255.255.255.0
ipv6 address 2001:DB8:0:20::1/64
ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPOOL
end
```

This interface configuration is for a Cisco IOS IPv6 router implementing stateful DHCPv6 on an external DHCP server:

```
ipv6 unicast-routing
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateful
ip address 192.168.20.1 255.255.255.0
ipv6 address 2001:DB8:0:20::1/64
ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp_relay destination 2001:DB8:0:20::2
end
```

Related Topics

Configuring IPv6 Snooping, on page 58
Configuring DHCP Pool , on page 62
Configuring Stateless Auto Address Configuration Without DHCP (CLI), on page 63
Configuring Stateless Auto Address Configuration With DHCP , on page 65
Configuring Stateful DHCP Locally, on page 66
Configuring Stateful DHCP Externally, on page 68

Static IP Address Assignment

Statically configured address on a client.

Router Solicitation

A Router Solicitation message is issued by a host controller to facilitate local routers to transmit Router Advertisement from which it can obtain information about local routing or perform Stateless Auto-configuration. Router Advertisements are transmitted periodically and the host prompts with an immediate Router Advertisement using a Router Solicitation such as - when it boots or following a restart operation.

Related Topics

Configuring IPv6 ND Suppress Policy, on page 59

Router Advertisement

A Router Advertisement message is issued periodically by a router or in response to a Router Solicitation message from a host. The information contained in these messages is used by hosts to perform Stateless Auto-configuration and to modify its routing table.

Related Topics

Configuring IPv6 ND Suppress Policy, on page 59

Neighbor Discovery

IPv6 Neighbor Discovery is a set of messages and processes that determine relationships between neighboring nodes. Neighbor Discovery replaces ARP, ICMP Router Discovery, and ICMP Redirect used in IPv4.

IPv6 Neighbor Discovery inspection analyzes neighbor discovery messages in order to build a trusted binding table database, and IPv6 neighbor discovery packets that do not comply are dropped. The neighbor binding table in the tracks each IPv6 address and its associated MAC address. Clients are expired from the table according to Neighbor Binding timers.

Related Topics

Configuring IPv6 ND Suppress Policy, on page 59

Neighbor Discovery Suppression

The IPv6 addresses of wireless clients are cached by the switch. When the switch receives an NS multicast looking for an IPv6 address, and if the target address is known to the switch and belongs to one of its clients, the switch will reply with an NA message on behalf of the client. The result of this process generates the equivalent of the Address Resolution Protocol (ARP) table of IPv4 but is more efficient - uses generally fewer messages.

Note The switch acts like proxy and respond with NA, only when the **ipv6 nd suppress** command is configured

If the switch does not have the IPv6 address of a wireless client, the switch will not respond with NA and forward the NS packet to the wireless side. To resolve this, an NS Multicast Forwarding knob is provided. If this knob is enabled, the switch gets the NS packet for the IPv6 address that it does not have (cache miss) and forwards it to the wireless side. This packet reaches the intended wireless client and the client replies with NA.

This cache miss scenario occurs rarely, and only very few clients which do not implement complete IPv6 stack may not advertise their IPv6 address during NDP.

Related Topics

Configuring IPv6 ND Suppress Policy, on page 59

RA Guard

IPv6 clients configure IPv6 addresses and populate their router tables based on IPv6 router advertisement (RA) packets. The RA guard feature is similar to the RA guard feature of wired networks. RA guard increases the security of the IPv6 network by dropping the unwanted or rogue RA packets that come from wireless clients. If this feature is not configured, malicious IPv6 wireless clients announce themselves as the router for the network often with high priority, which would take higher precedence over legitimate IPv6 routers.

RA-Guard also examines the incoming RA's and decides whether to switch or block them based solely on information found in the message or in the switch configuration. The information available in the frames received is useful for RA validation:

- Port on which the frame is received
- IPv6 source address
- Prefix list

The following configuration information created on the switch is available to RA-Guard to validate against the information found in the received RA frame:

- Trusted/Untrusted ports for receiving RA-guard messages
- Trusted/Untrusted IPv6 source addresses of RA-sender
- Trusted/Untrusted Prefix list and Prefix ranges
- Router Preference

RA guard occurs at the switch. You can configure the switch to drop RA messages at the switch. All IPv6 RA messages are dropped, which protects other wireless clients and upstream wired network from malicious IPv6 clients.

```
//Create a policy for RA Guard//
ipv6 nd raguard policy raguard-router
trusted-port
device-role router

//Applying the RA Guard Policy on port/interface//
interface tengigabitethernet1/0/1 (Katana)
interface gigabitethernet1/0/1 (Edison)

ipv6 nd raguard attach-policy raguard-router
```

Related Topics

Configuring RA Guard Policy, on page 55
Applying RA Guard Policy, on page 56
Configuring RA Throttle Policy (CLI), on page 57
Applying RA Throttle Policy on VLAN (CLI), on page 58

RA Throttling

RA throttling allows the controller to enforce limits to RA packets headed toward the wireless network. By enabling RA throttling, routers that send many RA packets can be trimmed to a minimum frequency that will still maintain an IPv6 client connectivity. If a client sends an RS packet, an RA is sent back to the client. This RA is allowed through the controller and unicasted to the client. This process ensures that the new clients or roaming clients are not affected by the RA throttling.

Related Topics

Configuring RA Guard Policy, on page 55
Applying RA Guard Policy, on page 56
Configuring RA Throttle Policy (CLI), on page 57
Applying RA Throttle Policy on VLAN (CLI), on page 58

Configuring RA Guard Policy

Configure RA Guard policy on the switch to add IPv6 client addresses and populate the router table based on IPv6 router advertisement packets.

To configuring RA guard policy, perform this procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 nd raguard policy raguard-router** **Example:** `Switch(config)# ipv6 nd raguard policy raguard-router`	Defines the RA guard policy name and enters RA guard policy configuration mode.
Step 4	**trustedport** **Example:** `Switch(config-ra-guard)# trustedport`	(Optional) Specifies that this policy is being applied to trusted ports.
Step 5	**device-role router** **Example:** `Switch(config-ra-guard)# device-role router`	Specifies the role of the device attached to the port.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Switch(config-ra-guard)# exit`	Exits RA guard policy configuration mode and returns to global configuration mode.

Related Topics

Prerequisites for IPv6 Client Address Learning, on page 49
RA Guard, on page 54
RA Throttling, on page 55
Applying RA Guard Policy, on page 56
Configuring RA Throttle Policy (CLI), on page 57
Applying RA Throttle Policy on VLAN (CLI), on page 58

Applying RA Guard Policy

Applying the RA Guard policy on the switch will block all the untrusted RA's.

To apply RA guard policy, perform this procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**interface tengigabitethernet 1/0/1** **Example:** `Switch(config)# interface tengigabitethernet 1/0/1`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**ipv6 nd raguard attach-policy raguard-router** **Example:** `Switch(config-if)# ipv6 nd raguard attach-policy raguard-router`	Applies the IPv6 RA Guard feature to a specified interface.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Switch(config-if)# exit`	Exits interface configuration mode.

Related Topics

Configuring RA Guard Policy, on page 55
RA Guard, on page 54
RA Throttling, on page 55
Configuring RA Throttle Policy (CLI), on page 57
Applying RA Throttle Policy on VLAN (CLI), on page 58

Configuring RA Throttle Policy (CLI)

Configure RA Throttle policy to allow the enforce the limits

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**ipv6 nd ra-throttler policy ra-throttler1** **Example:** `Switch(config)# ipv6 nd ra-throttler policy ra-throttler1`	Define the router advertisement (RA) throttler policy name and enter IPv6 RA throttle policy configuration mode.
Step 3	**throttleperiod500** **Example:** `Switch(config-nd-ra-throttle)# throttleperiod 500`	Configures the throttle period in an IPv6 RA throttler policy.
Step 4	**max-through10** **Example:** `Switch(config-nd-ra-throttle)# max-through 500`	Limits multicast RAs per VLAN per throttle period.
Step 5	**allow-atleast 5 at-most 10** **Example:** `Switch(config-nd-ra-throttle)# allow-atleast 5 at-most 10`	Limits the number of multicast RAs per device per throttle period in an RA throttler policy.

Related Topics

Configuring RA Guard Policy, on page 55
Applying RA Guard Policy, on page 56
RA Guard, on page 54
RA Throttling, on page 55
Applying RA Throttle Policy on VLAN (CLI), on page 58

Applying RA Throttle Policy on VLAN (CLI)

Applying the RA Throttle policy on a VLAN. By enabling RA throttling, routers that send many RA packets can be trimmed to a minimum frequency that will still maintain an IPv6 client connectivity.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**vlan configuration 1** **Example:** `Switch(config)# vlan configuration 1`	Configures a VLAN or a collection of VLANs and enters VLAN configuration mode.
Step 3	**ipv6 nd ra throttler attach-policy ra-throttler1** **Example:** `Switch(config-vlan)# ipv6 nd ra throttler attach-policy ra-throttler1`	Attaches an IPv6 RA throttler policy to a VLAN or a collection of VLANs.

Related Topics

Configuring RA Guard Policy, on page 55
Applying RA Guard Policy, on page 56
Configuring RA Throttle Policy (CLI), on page 57
RA Guard, on page 54
RA Throttling, on page 55

Configuring IPv6 Snooping

IPv6 snooping must always be enabled on the switch and the controller.

To configuring IPv6 snooping, perform this procedure:

Before you begin

Enable IPv6 on the client machine.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**vlan configuration 1** **Example:** `Switch(config)# vlan configuration 1`	Enters VLAN configuration mode.
Step 4	**ipv6 snooping** **Example:** `Switch(config-vlan)# ipv6 snooping`	Enables IPv6 snooping on the Vlan.
Step 5	**ipv6 nd suppress** **Example:** `Switch(config-vlan-config)# ipv6 nd suppress`	Enables the IPv6 ND suppress on the Vlan.
Step 6	**exit** **Example:** `Switch(config-vlan-config)# exit`	Saves the configuration and comes out of the Vlan configuration mode.

Related Topics

SLAAC Address Assignment, on page 50
Stateful DHCPv6 Address Assignment, on page 51

Configuring IPv6 ND Suppress Policy

The IPv6 neighbor discovery (ND) multicast suppress feature stops as many ND multicast neighbor solicit (NS) messages as possible by dropping them (and responding to solicitations on behalf of the targets) or converting them into unicast traffic. This feature runs on a layer 2 switch or a wireless controller and is used to reduce the amount of control traffic necessary for proper link operations.

When an address is inserted into the binding table, an address resolution request sent to a multicast address is intercepted, and the device either responds on behalf of the address owner or, at layer 2, converts the request into a unicast message and forwards it to its destination.

To configure IPv6 ND suppress policy, perform this procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 nd suppress policy** **Example:** `Switch(config)# ipv6 nd suppress policy`	Defines the ND suppress policy name and enters ND suppress policy configuration mode.

Related Topics

Router Solicitation, on page 53
Router Advertisement, on page 53
Neighbor Discovery, on page 53
Neighbor Discovery Suppression, on page 53

Configuring IPv6 Snooping on VLAN/PortChannel

Neighbor Discover (ND) suppress can be enabled or disabled on either the VLAN or a switchport.

To configure IPv6 snooping on VLAN/PortChannel, perform this procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Switch# configure terminal`	
Step 3	**vlan config901** **Example:** `Switch(config)# vlan config901`	Creates a VLAN and enter the VLAN configuration mode
Step 4	**ipv6 nd suppress** **Example:** `Switch(config-vlan)# ipv6 nd suppress`	Applies the IPv6 nd suppress on VLAN.
Step 5	**end** **Example:** `Switch(config-vlan)# end`	Exits vlan configuration mode and enters the global configuration mode.
Step 6	**interface gi1/0/1** **Example:** `Switch(config)# interface gi1/0/1`	Creates a gigabitethernet port interface.
Step 7	**ipv6 nd suppress** **Example:** `Switch(config-vlan)# ipv6 nd suppress`	Applies the IPv6 nd suppress on the interface.
Step 8	**end** **Example:** `Switch(config-vlan)# end`	Exits vlan configuration mode and enters the global configuration mode.

Configuring IPv6 on Interface

To configure IPv6 on an interface, perform this procedure:

Before you begin

Enable IPv6 on the client and IPv6 support on the wired infrastructure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**interface vlan 1** **Example:** `Switch(config)# interface vlan 1`	Creates a interface and enters interface configuration mode.

Step 4	**ip address fe80::1 link-local**
	Example:
	`Switch(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Switch(config-if)# ipv6 address fe80::1 link-local`
	`Switch(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Switch(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		Configures IPv6 address on the interface using the link-local option.

Step 5	**ipv6 enable** **Example:** `Switch(config)# ipv6 enable`	(Optional) Enables IPv6 on the interface.
Step 6	**end** **Example:** `Switch(config)# end`	Exits from the interface mode.

Configuring DHCP Pool

To configure DHCP Pool on an interface, perform this procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Switch# configure terminal`	
Step 3	**ipv6 dhcp pool `Vlan21`** **Example:** `Switch(config)# ipv6 dhcp pool vlan1`	Enters the configuration mode and configures the IPv6 DHCP pool on the Vlan.
Step 4	**address prefix `2001:DB8:0:1:FFFF:1234::/64` lifetime `300 10`** **Example:** `Switch(config-dhcpv6)# address prefix 2001:DB8:0:1:FFFF:1234::/64 lifetime 300 10`	Enters the configuration-dhcp mode and configures the address pool and its lifetime on a Vlan.
Step 5	**dns-server `2001:100:0:1::1`** **Example:** `Switch(config-dhcpv6)# dns-server 2001:20:21::1`	Configures the DNS servers for the DHCP pool.
Step 6	**domain-name `example.com`** **Example:** `Switch(config-dhcpv6)# domain-name example.com`	Configures the domain name to complete unqualified host names.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

SLAAC Address Assignment, on page 50
Stateful DHCPv6 Address Assignment, on page 51

Configuring Stateless Auto Address Configuration Without DHCP (CLI)

To configure stateless auto address configuration without DHCP, perform this procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
	`Switch> enable`	
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**interface vlan 1** **Example:** `Switch(config)# interface vlan 1`	Creates a interface and enters interface configuration mode.

Step 4	**ip address fe80::1 link-local**
	Example:
	`Switch(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Switch(config-if)# ipv6 address fe80::1 link-local`
	`Switch(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Switch(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		Configures IPv6 address on the interface using the link-local option.

Step 5	**ipv6 enable** **Example:** `Switch(config)# ipv6 enable`	(Optional) Enables IPv6 on the interface.

Step 6	**no ipv6 nd managed-config-flag**
	Example:
	`Switch(config)# interface vlan 1`
	`Switch(config-if)# no ipv6 nd managed-config-flag`
		Ensures the attached hosts do not use stateful autoconfiguration to obtain addresses.

Step 7	**no ipv6 nd other-config-flag** **Example:** `Switch(config-if)# no ipv6 nd other-config-flag`	Ensures the attached hosts do not use stateful autoconfiguration to obtain non-address options from DHCP (domain etc).
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

SLAAC Address Assignment, on page 50
Stateful DHCPv6 Address Assignment, on page 51

Configuring Stateless Auto Address Configuration With DHCP

To configure stateless auto address configuration with DHCP, perform this procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**interface vlan 1** **Example:** `Switch(config)# interface vlan 1`	Creates a interface and enters interface configuration mode.

Step 4	**ip address fe80::1 link-local**
	Example:
	`Switch(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Switch(config-if)# ipv6 address fe80::1 link-local`
	`Switch(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Switch(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		Configures IPv6 address on the interface using the link-local option.

Step 5	**ipv6 enable** **Example:** `Switch(config)# ipv6 enable`	(Optional) Enables IPv6 on the interface.

Step 6	**no ipv6 nd managed-config-flag**
	Example:
	`Switch(config)# interface vlan 1`
	`Switch(config-if)# no ipv6 nd managed-config-flag`
		Ensures the attached hosts do not use stateful autoconfiguration to obtain addresses.

Step 7	**ipv6 nd other-config-flag** **Example:** `Switch(config-if)# no ipv6 nd other-config-flag`	Ensures the attached hosts do not use stateful autoconfiguration to obtain non-address options from DHCP (domain etc).

	Command or Action	Purpose
Step 8	**end** **Example:** `Switch(config)# end`	Exits from the interface mode.

Related Topics

SLAAC Address Assignment, on page 50
Stateful DHCPv6 Address Assignment, on page 51

Configuring Stateful DHCP Locally

This interface configuration is for a Cisco IOS IPv6 router implementing stateful DHCPv6 on a local Switch

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 unicast-routing** **Example:** `Switch(config)# ipv6 unicast-routing`	Configures IPv6 for unicasting.
Step 4	**ipv6 dhcp pool IPv6_DHCPPOOL** **Example:** `Switch (config)# ipv6 dhcp pool IPv6_DHCPPOOL`	Enters the configuration mode and configures the IPv6 DHCP pool on the VLAN.
Step 5	**address prefix 2001:DB8:0:1:FFFF:1234::/64** **Example:** `Switch (config-dhcpv6)# address prefix 2001:DB8:0:1:FFFF:1234::/64`	Specifies the address range to provide in the pool.
Step 6	**dns-server 2001:100:0:1::1** **Example:**	Provides the DNS server option to DHCP clients.

	Command or Action	Purpose
	`Switch (config-dhcpv6)# dns-server 2001:100:0:1::1`	
Step 7	**domain-name `example.com`** **Example:** `Switch (config-dhcpv6)# domain-name example.com`	Provides the domain name option to DHCP clients.
Step 8	**exit** **Example:** `Switch (config-dhcpv6)# exit`	Returns to the previous mode.
Step 9	**interface `vlan1`** **Example:** `Switch (config)# interface vlan 1`	Enters the interface mode to configure the stateful DHCP.
Step 10	**description IPv6-DHCP-Stateful** **Example:** `Switch (config-if)# description IPv6-DHCP-Stateful`	Enter description for the stateful IPv6 DHCP.
Step 11	**ipv6 address `2001:DB8:0:20::1/64`** **Example:** `Switch (config-if)# ipv6 address 2001:DB8:0:20::1/64`	Enters the IPv6 address for the stateful IPv6 DHCP.
Step 12	**ip address `192.168.20.1 255.255.255.0`** **Example:** `Switch (config-if)# ip address 192.168.20.1 255.255.255.0`	Enters the IPv6 address for the stateful IPv6 DHCP.
Step 13	**ipv6 nd prefix `2001:db8::/64` no-advertise** **Example:** `Switch (config-if)# ipv6 nd prefix 2001:db8::/64 no-advertise`	Configures the IPv6 routing prefix advertisement that must not be advertised.
Step 14	**ipv6 nd managed-config-flag** **Example:** `Switch (config-if)# ipv6 nd managed-config-flag`	Configures IPv6 interfaces neighbor discovery to allow the hosts to uses DHCP for address configuration.
Step 15	**ipv6 nd other-config-flag** **Example:** `Switch (config-if)# ipv6 nd other-config-flag`	Configures IPv6 interfaces neighbor discovery to allow the hosts to uses DHCP for non-address configuration.

	Command or Action	Purpose
Step 16	**ipv6 dhcp server IPv6_DHCPPOOL** **Example:** `Switch (config-if)# ipv6 dhcp server IPv6_DHCPPOOL`	Configures the DHCP server on the interface.

Related Topics

SLAAC Address Assignment, on page 50
Stateful DHCPv6 Address Assignment, on page 51

Configuring Stateful DHCP Externally

This interface configuration is for a Cisco IOS IPv6 router implementing stateful DHCPv6 on an external DHCP server.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 unicast-routing** **Example:** `Switch(config)# ipv6 unicast-routing`	Configures the IPv6 for unicasting.
Step 4	**dns-server 2001:100:0:1::1** **Example:** `Switch(config-dhcpv6)# dns-server 2001:100:0:1::1`	Provides the DNS server option to DHCP clients.
Step 5	**domain-name example.com** **Example:** `Switch(config-dhcpv6)# domain-name example.com`	Provides the domain name option to DHCP clients.
Step 6	**exit** **Example:**	Returns to the previous mode.

	Command or Action	Purpose
	`Switch(config-dhcpv6)# exit`	
Step 7	**interface vlan1** **Example:** `Switch(config)# interface vlan 1`	Enters the interface mode to configure the stateful DHCP.
Step 8	**description IPv6-DHCP-Stateful** **Example:** `Switch(config-if)# description IPv6-DHCP-Stateful`	Enter description for the stateful IPv6 DHCP.
Step 9	**ipv6 address 2001:DB8:0:20::1/64** **Example:** `Switch(config-if)# ipv6 address 2001:DB8:0:20::1/64`	Enters the IPv6 address for the stateful IPv6 DHCP.
Step 10	**ip address 192.168.20.1 255.255.255.0** **Example:** `Switch(config-if)# ip address 192.168.20.1 255.255.255.0`	Enters the IPv6 address for the stateful IPv6 DHCP.
Step 11	**ipv6 nd prefix 2001:db8::/64 no-advertise** **Example:** `Switch(config-if)# ipv6 nd prefix 2001:db8::/64 no-advertise`	Configures the IPv6 routing prefix advertisement that must not be advertised.
Step 12	**ipv6 nd managed-config-flag** **Example:** `Switch(config-if)# ipv6 nd managed-config-flag`	Configures IPv6 interfaces neighbor discovery to allow the hosts to uses DHCP for address configuration.
Step 13	**ipv6 nd other-config-flag** **Example:** `Switch(config-if)# ipv6 nd other-config-flag`	Configures IPv6 interfaces neighbor discovery to allow the hosts to uses DHCP for non-address configuration.
Step 14	**ipv6 dhcp_relaydestination 2001:DB8:0:20::2** **Example:** `Switch(config-if)# ipv6 dhcp_relay destination 2001:DB8:0:20::2`	Configures the DHCP server on the interface.

Related Topics

SLAAC Address Assignment, on page 50
Stateful DHCPv6 Address Assignment, on page 51

Monitoring IPv6 Clients (GUI)

To view the IPv6 clients associated with the Switch

Procedure

Select **Monitor** > **Clients**

The Clients page is displayed. The Clients page contains the following details:

- Client MAC Address— Displays the MAC address of the client.
- AP Name— Displays the access point name to which the client is connected to.
- WLAN— Displays the WLAN associated with the client.
- State— Displays the client authentication.
- Protocol— Displays the protocol used.

To view the client related general details, click the **Client MAC Address** parameter in the Clients page. The **Client > Detail** page displays IPv6 addresses of the client under the **General** tab.

Verifying IPv6 Address Learning Configuration

This example displays the output of the **show ipv6 dhcp pool** command. This command displays the IPv6 service configuration on the switch. The vlan 21 configured pool detail displays 6 clients that are currently using addresses from the pool.

Procedure

	Command or Action	Purpose

Step 1	**show ipv6 dhcp pool**
	Example:
	`Switchshow ipv6 dhcp pool`
	`DHCPv6 pool: vlan21`
	`Address allocation prefix:`
	`2001:DB8:0:1:FFFF:1234::/64 valid 86400`
	`preferred 86400 (6 in use, 0 conflicts)`
	`DNS server: 2001:100:0:1::1`
	`Domain name: example.com`
	`Active clients: 6`
		Displays the IPv6 service configuration on the switch.

Additional References

Related Documents

Related Topic	Document Title
IPv6 command reference	*IPv6 Command Reference (Catalyst 3850 Switches)IPv6 Command Reference (Cisco WLC 5700 Series)*
IP command reference	*IP Command Reference (Catalyst 3850 Switches)IP Command Reference (Cisco WLC 5700 Series)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

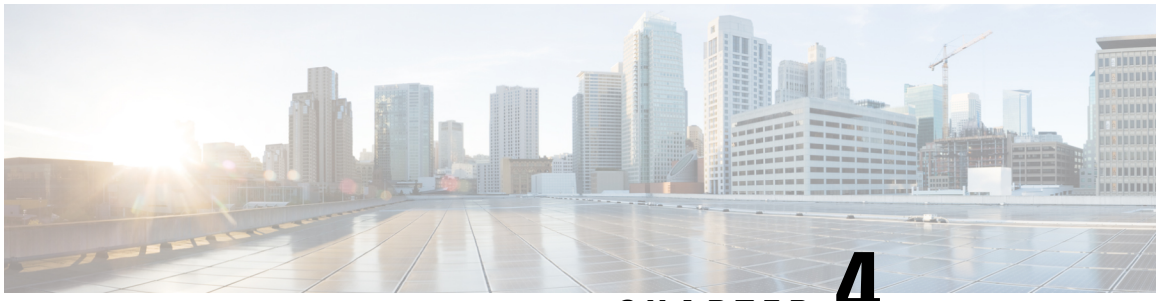
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for IPv6 Client Address Learning

This table lists the features in this module and provides links to specific configuration information:

Feature	Release	Modification
IPv6 Client Address Learning Functionality	Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 4

Configuring IPv6 WLAN Security

Prerequisites for IPv6 WLAN Security

A client VLAN must be mapped to the WLAN configured on the switch

Restrictions for IPv6 WLAN Security

RADIUS Server Support

- If multiple RADIUS servers are configured for redundancy, the user database must be identical in all the servers for the backup to work properly.

Radius ACS Support

- You must configure RADIUS on both your Cisco Secure Access Control Server (ACS) and your switch
- RADIUS is supported on Cisco Secure ACS version 3.2 and later releases.

Information About IPv6 WLAN Security

Information About RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol that provides centralized security for users attempting to gain management access to a network. It serves as a back-end database similar to Local EAP and provides authentication and accounting services.

- Authentication—The process of verifying users when they attempt to log into the switch

  Users must enter a valid username and password for the switch to authenticate users to the RADIUS server. If multiple databases are configured, then specify the sequence in which the backend database must be tried.

- Accounting— The process of recording user actions and changes.

  Whenever a user successfully executes an action, the RADIUS accounting server logs the changed attributes, the user ID of the person who made the change, the remote host where the user is logged in, the date and time when the command was executed, the authorization level of the user, and a description of the action performed and the values provided. If the RADIUS accounting server is unreachable, the users can continue their sessions uninterrupted.

User Datagram Protocol— RADIUS uses User Datagram Protocol (UDP) for its transport. It maintains a database and listens on UDP port 1812 for incoming authentication requests and UDP port 1813 for incoming accounting requests. The switch, which requires access control, acts as the client and requests AAA services from the server. The traffic between the switch and the server is encrypted by an algorithm defined in the protocol and a shared secret key configured on both devices.

Configures multiple RADIUS accounting and authentication servers. For example, you can have one central RADIUS authentication server but several RADIUS accounting servers in different regions. If you configure multiple servers of the same type and the first one fails or becomes unreachable, the controller automatically tries the second one, then the third one if necessary, and so on.

When RADIUS method is configured for the WLAN, the switch will use the RADIUS method configured for the WLAN. When the WLAN is configured to use local EAP, the RADIUS method configured on the WLAN points to Local. The WLAN must also be configured with the name of the local EAP profile to use.

If no RADIUS method is configured in the WLAN, the switch will use the default RADIUS method defined in global mode.

Information About Local EAP

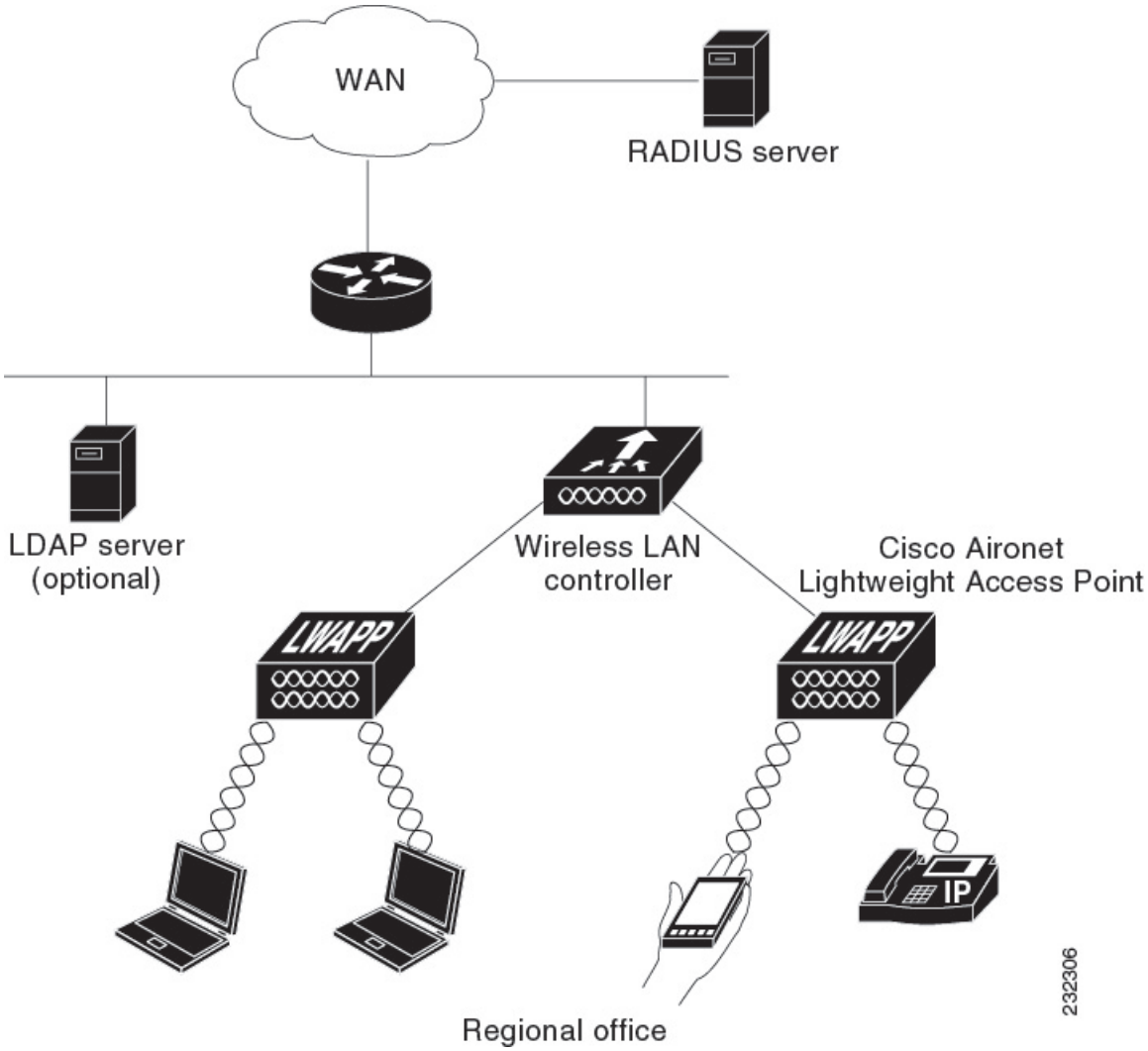
Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that maintain connectivity to wireless clients when the back-end system is disrupted or the external authentication server goes down. When you enable local EAP, the switch serves as the authentication server and the local user database, which removes dependence on an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP back-end database to authenticate users. Local EAP supports LEAP, EAP-FAST, EAP-TLS, PEAPv0/MSCHAPv2, and PEAPv1/GTC authentication between the controller and wireless clients.

Without an EAP profile name being provided, or if a name was provided for an EAP profile that does not exist, then EAP by default allows no EAP method for local authentication.

Note The LDAP back-end database supports these local EAP methods: EAP-TLS, EAP-FAST/GTC, and PEAPv1/GTC. LEAP, EAP-FAST/MSCHAPv2, and PEAPv0. MSCHAPv2 is supported only if the LDAP server is set up to return a clear-text password.

Note Switch support Local EAP authentication against external LDAP databases such as Microsoft Active Directory and Novell's eDirectory. For more information about configuring the controller for Local EAP authentication against Novell's eDirectory, see the Configure Unified Wireless Network for Authentication Against Novell's eDirectory Database whitepaper.

Figure 4: Local EAP Example



Related Topics

Creating a Local User, on page 76
Creating an Client VLAN and Interface, on page 76
Configuring an EAP Profile, on page 77
Creating a Client VLAN, on page 88
Creating 802.1x WLAN Using an External RADIUS Server, on page 89

How to Configure IPv6 WLAN Security

Configuring Local Authentication

Creating a Local User

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 2	**username aaa_test** **Example:** `Switch(config)# username aaa_test`	Creates a username.
Step 3	**password 0 aaa_test** **Example:** `Switch(config)# usernameaaa_test password 0 aaa_test`	Assigns a password for the username.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit the global configuration mode.

```
Switch# configure terminal
Switch(config)# username aaa_test password 0 aaa_test
Switch(config)# end
```

Related Topics

Information About IPv6 WLAN Security, on page 73

Creating an Client VLAN and Interface

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 2	**vlan**	Creates a VLAN.

	Command or Action	Purpose
	Example: `Switch(config)# vlan 137`	
Step 3	**exit** **Example:** `Switch (config-vlan)# exit`	Exits VLAN configuration mode.
Step 4	**interface vlan `vlan_ID`** **Example:** `Switch (config)# interface vlan 137`	Associates the VLAN to an interface.
Step 5	**ip address** **Example:** `Switch(config-if)# ip address 10.7.137.10 255.255.255.0`	Assigns an IP address to the VLAN interface.
Step 6	**ipv6 address** **Example:** `Switch(config-if)#ipv6 address 2001:db8::20:1/64`	Assigns an IPv6 address to the VLAN interface.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit the global configuration mode.

Example

```
Switch# configure terminal
Switch(config)# vlan 137
Switch(config-vlan)#exit
Switch(config)#interface vlan 137
Switch(config-if)#ip address 10.7.137.10 255.255.255.0
Switch(config-if)#ipv6 address 2001:db8::20:1/64
Switch(config-if)#end
```

Related Topics

Information About IPv6 WLAN Security, on page 73

Configuring an EAP Profile

Procedure

	Command or Action	Purpose
Step 1	**eap profile `name`** **Example:** `Switch(config)# eap profile wcm_eap_prof`	Creates an EAP profile.

	Command or Action	Purpose
Step 2	**method leap** **Example:** `Switch(config-eap-profile)# method leap`	Configures EAP-LEAP method on the profile.
Step 3	**method tls** **Example:** `Switch(config-eap-profile)# method tls`	Configures EAP-TLS method on the profile.
Step 4	**method peap** **Example:** `Switch(config-eap-profile)# method peap`	Configures PEAP method on the profile.
Step 5	**method fast** **Example:** `Switch(config-eap-profile)# method fast`	Configures EAP-FAST method on the profile.
Step 6	**method mschapv2** **Example:** `Switch(config-eap-profile)# method mschapv2`	Configures EAP-MSCHAPV2 method on the profile.
Step 7	**method md5** **Example:** `Switch(config-eap-profile)# method md5`	Configures EAP-MD5 method on the profile.
Step 8	**method gtc** **Example:** `Switch(config-eap-profile)# method gtc`	Configures EAP-GTC method on the profile.

Step 9	**method fast profile `my-fast`**
	Example:
	`Switch(config-eap-profile)# eap method fast profile my-fast`
	`Switch (config-eap-profile)#description my_local eap profile`
		Creates a EAP profile named my-fast.

Step 10	**description `my_local eap profile`** **Example:** `Switch (config-eap-profile)#description my_local eap profile`	Provides a description for the local profile.
Step 11	**exit** **Example:** `Switch (config-eap-profile)# exit`	Exits the eap-profile configuration mode.

	Command or Action	Purpose
Step 12	**eap method fast profile myFast** **Example:** `Switch (config)# eap method fast profile myFast`	Configures the EAP method profile.

Step 13	**authority-id** `[identity|information]`
	Example:
	`Switch(config-eap-method-profile)# authority-id identity my_identity`
	`Switch(config-eap-method-profile)#authority-id information my_information`
		Configure the authority ID and information for the EAP method profile.

Step 14	**local-key 0 key-name** **Example:** `Switch(config-eap-method-profile)# local-key 0 test`	Configures the local server key.
Step 15	**pac-password 0 password** **Example:** `Switch(config-eap-method-profile)# pac-password 0 test`	Configures the PAC password for manual PAC provisioning.
Step 16	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit the global configuration mode.

Example

```
Switch(config)#eap profile wcm_eap_prof
Switch(config-eap-profile)#method leap
Switch(config-eap-profile)#method tls
Switch(config-eap-profile)#method peap

Switch(config-eap-profile)#method mschapv2
Switch(config-eap-profile)#method md5
Switch(config-eap-profile)#method gtc
Switch(config-eap-profile)#eap method fast profile my-fast

Switch (config-eap-profile)#description my_local eap profile
Switch(config-eap-profile)# exit
Switch (config)# eap method fast profile myFast
Switch(config-eap-method-profile)#authority-id identity my_identity
Switch(config-eap-method-profile)#authority-id information my_information
Switch(config-eap-method-profile)#local-key 0 test
Switch(config-eap-method-profile)#pac-password 0 test
Switch(config-eap-method-profile)# end
```

Related Topics

Information About IPv6 WLAN Security, on page 73

Creating a Local Authentication Model

Procedure

	Command or Action	Purpose
Step 1	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Creates a AAA authentication model.
Step 2	**authentication dot1x default local** **Example:** `Switch(config)# aaa authentication dot1x default local`	Implies that the dot1x must use the default local RADIUS when no other method is found.
Step 3	**dot1x method_list local** **Example:** `Switch(config)# aaa authentication dot1x wcm_local local`	Assigns the local authentication for wcm_local method list.
Step 4	**aaa authentication dot1x dot1x_name local** **Example:** `Switch(config)# aaa authentication dot1x aaa_auth local`	Configures the local authentication for the dot1x method.
Step 5	**aaa authorization credential-download name local** **Example:** `Switch(config)# aaa authorization credential-download wcm_author local`	Configures local database to download EAP credentials from Local/RADIUS/LDAP.
Step 6	**aaa local authentication auth-name authorization authorization-name** **Example:** `Switch(config)# aaa local authentication wcm_local authorization wcm_author`	Selects local authentication and authorization.
Step 7	**session ID** **Example:** `Switch(config)# aaa session-id common`	Configures a session ID for AAA.
Step 8	**dot1x system-auth-control** **Example:** `Switch(config)# dot1x system-auth-control`	Enables dot.1x system authentication control.

Example

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default local
Switch(config)# aaa authentication dot1x wcm-local local
Switch(config)# aaa authentication dot1x aaa_auth local
Switch(config)# aaa authorization credential-download wcm_author local
Switch(config)# aaa local authentication wcm_local authorization wcm_author
Switch(config)# aaa session-id common
Switch(config)# dot1x system-auth-control
```

Creating a Client WLAN

Note This example uses 802.1x with dynamic WEP. You can use any other security mechanism supported by the wireless client and configurable on the switch

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 2	**wlan wlan name <identifier> SSID** **Example:** `Switch(config)# wlan wlanProfileName 1 ngwcSSID`	Creates a WLAN.
Step 3	**broadcast-ssid** **Example:** `Switch(config-wlan)# broadcast-ssid`	Configures to broadcast the SSID on a WLAN.
Step 4	**no security wpa** **Example:** `Switch(config-wlan)# no security wpa`	Disables the wpa for WLAN to enable 802.1x.
Step 5	**security dot1x** **Example:** `Switch(config-wlan)# security dot1x`	Configures the 802.1x encryption security for the WLAN.
Step 6	**security** dot1x authentication-list *wcm-local* **Example:** `Switch(config-wlan)# security dot1x authentication-list wcm-local`	Configures the server group mapping to the WLAN for dot1x authentication.

	Command or Action	Purpose
Step 7	**local-auth wcm_eap_prof** **Example:** `Switch (config-wlan)# local-auth wcm_eap_profile`	Configures the eap profile on the WLAN for local authentication.
Step 8	**client vlan** *137* **Example:** `Switch(config-wlan)# client vlan 137`	Associates the VLAN to a WLAN.
Step 9	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Enables the WLAN.
Step 10	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit the global configuration mode.

Example

```
Switch# config terminal
Switch(config)#wlan wlanProfileName 1 ngwcSSID
Switch(config-wlan)#broadcast-ssid
Switch(config-wlan)#no security wpa
Switch(config-wlan)#security dot1x
Switch(config-wlan)#security dot1x authentication-list wcm-local
Switch (config-wlan)# local-auth wcm_eap_prof
Switch(config-wlan)#client vlan 137
Switch(config-wlan)#no shutdown
Switch(config-wlan)#end
Switch#
```

Related Topics

Creating Client VLAN for WPA2+AES, on page 83

Configuring Local Authentication with WPA2+AES

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 2	**aaa new model** **Example:** `Switch(config)# aaa new-model`	Creates a AAA authentication model.

	Command or Action	Purpose
Step 3	**dot1x system-auth-control** **Example:** `Switch(config)# dot1x system-auth-control`	Enables dot1x system authentication control.
Step 4	**aaa authentication dot1x default local** **Example:** `Switch(config)# aaa authentication dot1x default local`	Configures the local authentication for the default dot1x method.
Step 5	**aaa local authorization credential-download default local** **Example:** `Switch(config)# aaa authorization credential-download default local`	Configures default database to download EAP credentials from local server.
Step 6	**aaa local authentication default authorization default** **Example:** `Switch(config)# aaa local authentication default authorization default`	Selects the default local authentication and authorization.
Step 7	**eap profile wcm_eap_profile** **Example:** `Switch(config)#eap profile wcm_eap_profile`	Creates an EAP profile.
Step 8	**method leap** **Example:** `Switch(config)# method leap`	Configures EAP-LEAP method on the profile.
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit the global configuration mode.

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# dot1x system-auth-control
Switch(config)# aaa authentication dot1x default local
Switch(config)# aaa authorization credential-download default local
Switch(config)# aaa local authentication default authorization default
Switch(config)#eap profile wcm_eap_profile
Switch(config)# method leap
Switch(config)# end
```

Creating Client VLAN for WPA2+AES

Create a VLAN for the WPA2+AES type of local authentication. This VLAN is later mapped to a WLAN.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 2	**vlan vlan_ID** **Example:** `Switch (config)# vlan 105`	Creates a VLAN.
Step 3	**exit** **Example:** `Switch (config-vlan)# exit`	Exits from the VLAN mode.
Step 4	**interface** vlan **vlan_ID** **Example:** `Switch(config)# interface vlan 105`	Associates the VLAN to the interface.
Step 5	**ip address** **Example:** `Switch(config-if)# ip address 10.8.105.10 255.255.255.0`	Assigns IP address to the VLAN interface.
Step 6	**ipv6 address** **Example:** `Switch(config-if)#ipv6 address 2001:db8::10:1/64`	Assigns IPv6 address to the VLAN interface.
Step 7	**exit** **Example:** `Switch (config-if)# exit`	Exits from the interface mode.

```
Switch# configure terminal
Switch(config)# vlan105
Switch (config-vlan)# exit
Switch (config)# interface vlan 105
Switch(config-if)#ip address 10.8.105.10 255.255.255.0
Switch(config-if)#ipv6 address 2001:db8::10:1/64
Switch(config-if)#exit
Switch(config)#
```

Related Topics

Creating a Client WLAN , on page 81

Creating WLAN for WPA2+AES

Create a WLAN and map it to the client VLAN created for WPA2+AES.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.

Step 2	**wlan wpas2-aes-wlan 1 wpas2-aes-wlan**
	Example:
	`Switch(config)#wlan wpa2-aes-wlan 1 wpa2-aes-wlan`
	`Switch(config-wlan)#`
		Creates a WLAN.

Step 3	**client vlan 105**
	Example:
	`Switch(config-wlan)#client vlan 105`
	`Switch(config-wlan)#`
		Maps the WLAN to the client VLAN.

Step 4	**local-auth wcm_eap_profile** **Example:** `Switch(config-wlan)#local-auth wcm_eap_profile`	Creates and sets the EAP profile on the WLAN.
Step 5	**security dot1x authentication-list default** **Example:** `Switch(config-wlan)#security dot1x authentication-list default`	Uses the default dot1x authentication list.

Step 6	**no shutdown**
	Example:
	`Switch(config-wlan)#no shutdown`
	`Switch(config-wlan)#`
		Enables the WLAN.

Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

```
Switch# configure terminal
Switch(config)#wlan wpa2-aes-wlan 1 wpa2-aes-wlan
Switch(config-wlan)#client vlan 105
Switch(config-wlan)#local-auth wcm_eap_profile
Switch(config-wlan)#security dot1x authentication-list default
Switch(config-wlan)#no shutdown
Switch(config-wlan)# exit
```

Configuring External RADIUS Server

Configuring RADIUS Authentication Server Host

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 2	**radius server One** **Example:** `Switch (config)# radius server One`	Creates a radius server.
Step 3	**address ipv4 address auth-portauth_port_number acct-port acct_port_number** **Example:** `Switch (config-radius-server)# address ipv4 10.10.10.10 auth-port 1812 acct-port 1813`	Configures the IPv4 address for the radius server.
Step 4	**address ipv6 address auth-portauth_port_number acct-port acct_port_number** **Example:** `Switch (config-radius-server)# address ipv6 2001:db8::25:2 auth-port 1812 acct-port 1813`	Configures the IPv6 address for the radius server.
Step 5	**key 0cisco** **Example:** `Switch (config-radius-server)# key 0 cisco`	**exit**
Step 6	**Example:** `Switch (config-radius-server)# exit`	Exits from the radius server mode.

```
Switch# configure terminal
Switch (config)# radius server One
Switch (config-radius-server)# address ipv4 10.10.10.10 auth-port 1812 acct-port 1813
Switch (config-radius-server)# address ipv6 2001:db8::25:2 auth-port 1812 acct-port 1813
Switch (config-radius-server)# key 0 cisco
Switch (config-radius-server)#exit
```

Related Topics

Configuring RADIUS Authentication Server Group , on page 87

Configuring RADIUS Authentication Server Group

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 2	**aaa new-model** **Example:** `Switch(config)#aaa new-model`	Creates a AAA authentication model.

Step 3	**aaa group server radius wcm_rad**
	Example:
	`Switch(config)# aaa group server radius wcm_rad`
	`Switch(config-sg-radius)#`
		Creates an radius server-group.

Step 4	**server <ip address>auth-port1812acct-port1813**
	Example:
	`Switch(config-sg-radius)# server One auth-port 1812 acct-port 1813`
	`Switch(config-sg-radius)# server Two auth-port 1812 acct-port 1813`
	`Switch(config-sg-radius)# server Three auth-port 1812 acct-port 1813`
		Adds servers to the radius group created in Step 3. Configures the UDP port for RADIUS accounting server and authentication server.

Step 5	**aaa authentication dot1x method_list group wcm_rad** **Example:** `Switch(config)# aaa authentication dot1x method_list group wcm_rad`	Maps the method list to the radius group.
Step 6	**dot1x system-auth-control** **Example:** `Switch(config)# dot1x system-auth-control`	Enables the system authorization control for the radius group.
Step 7	**aaa session-idcommon** **Example:** `Switch(config)# aaa session-id common`	Ensures that all session IDs information sent out, from the radius group, for a given call are identical.

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa group server radius wcm_rad
Switch(config-sg-radius)# server One auth-port 1812 acct-port 1813
Switch(config-sg-radius)# server Two auth-port 1812 acct-port 1813
Switch(config-sg-radius)# server Three auth-port 1812 acct-port 1813
Switch(config)# aaa authentication dot1x method_list group wcm_rad
```

```
Switch(config)# dot1x system-auth-control
Switch(config)# aaa session-id common
Switch(config)#
```

Related Topics

Configuring RADIUS Authentication Server Host , on page 86

Creating a Client VLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 2	**vlan 137** **Example:** `Switch(config)# vlan 137`	Creates a VLAN and associate it to the interface.
Step 3	**exit** **Example:** `Switch (config-vlan)# exit`	Exits from the VLAN mode.
Step 4	**interface vlan 137** **Example:** `Switch (config)# interface vlan 137`	Assigns a VLAN to an interface.
Step 5	**ip address 10.7.137.10 255.255.255.0** **Example:** `Switch(config-if)# ip address 10.7.137.10 255.255.255.0`	Assigns an IPv4 address to the VLAN interface.
Step 6	**ipv6 address 2001:db8::30:1/64** **Example:** `Switch(config-if)# ipv6 address 2001:db8::30:1/64`	Assigns an IPv6 address to the VLAN interface.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

```
Switch# configure terminal
Switch(config)# vlan137
Switch(config-vlan)# exit
Switch(config)# interface vlan137
Switch(config-if)# ip address 10.7.137.10 255.255.255.0
```

```
Switch(config-if)# ipv6 address 2001:db8::30:1/64
Switch(config-if)# end
```

Related Topics

Information About IPv6 WLAN Security, on page 73
Creating 802.1x WLAN Using an External RADIUS Server, on page 89

Creating 802.1x WLAN Using an External RADIUS Server

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 2	**wlan ngwc-1x<ssid>ngwc-1x** **Example:** `Switch(config)# wlan ngwc_8021x 2 ngwc_8021x`	Creates a new WLAN for 802.1x authentication.
Step 3	**broadcast-ssid** **Example:** `Switch(config-wlan)# broadcast-ssid`	Configures to broadcast the SSID on WLAN.
Step 4	**no security wpa** **Example:** `Switch(config-wlan)# no security wpa`	Disables the WPA for WLAN to enable 802.1x.
Step 5	**security dot1x** **Example:** `Switch(config-wlan)# security dot1x`	Configures the 802.1x encryption security for the WLAN.
Step 6	**security dot1x authentication-list wcm-rad** **Example:** `Switch(config-wlan)# security dot1x authentication-list wcm-rad`	Configures the server group mapping to the WLAN for dot1x authentication.
Step 7	**client vlan 137** **Example:** `Switch(config-wlan)# client vlan 137`	Associates the VLAN to a WLAN.
Step 8	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Enables the WLAN.

	Command or Action	Purpose
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit the global configuration mode.

Example

```
Switch# configure terminal
Switch(config)#wlan ngwc_8021x 2 ngwc_8021x
Switch(config-wlan)# broadcast-ssid
Switch(config-wlan)# no security wpa
Switch(config-wlan)# security dot1x
Switch(config-wlan)# security dot1x authentication-list wcm-rad
Switch(config-wlan)# client vlan 137
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

Related Topics

Creating a Client VLAN, on page 88
Information About IPv6 WLAN Security, on page 73

Additional References

Related Documents

Related Topic	Document Title
IPv6 command reference	*IPv6 Command Reference (Catalyst 3850 Switches)IPv6 Command Reference (Cisco WLC 5700 Series)*
WLAN command reference	*WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
WLAN configuration	*WLAN Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)WLAN Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

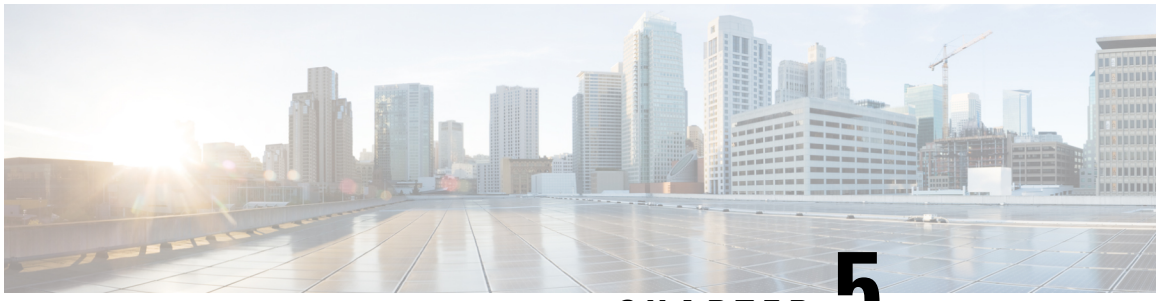
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for IPv6 WLAN Security

This table lists the features in this module and provides links to specific configuration information:

Feature	Release	Modification
IPv6 WLAN Security Functionality	Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 5

Configuring IPv6 ACL

Prerequisites for Configuring IPv6 ACL

You can filter IP Version 6 (IPv6) traffic by creating IPv6 access control lists (ACLs) and applying them to interfaces similarly to the way that you create and apply IP Version 4 (IPv4) named ACLs. You can also create and apply input router ACLs to filter Layer 3 management traffic when the switch is running the IP base feature set.

Related Topics

Creating an IPv6 ACL, on page 97

Restrictions for Configuring IPv6 ACL

With IPv4, you can configure standard and extended numbered IP ACLs, named IP ACLs, and MAC ACLs. IPv6 supports only named ACLs.

The switch supports most of the Cisco IOS-supported IPv6 ACLs with some exceptions:

- The switch does not support matching on these keywords: **flowlabel**, **routing header**, and **undetermined-transport**.
- The switch does not support reflexive ACLs (the **reflect** keyword).
- The switch does not apply MAC-based ACLs on IPv6 frames.
- When configuring an ACL, there is no restriction on keywords entered in the ACL, regardless of whether or not they are supported on the platform. When you apply the ACL to an interface that requires hardware

forwarding (physical ports or SVIs), the switch checks to determine whether or not the ACL can be supported on the interface. If not, attaching the ACL is rejected.

- If an ACL is applied to an interface and you attempt to add an access control entry (ACE) with an unsupported keyword, the switch does not allow the ACE to be added to the ACL that is currently attached to the interface

Information About IPv6 ACL

An access control list (ACL) is a set of rules used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the controller). ACLs are configured on the switchnd applied to the management interface, the AP-manager interface, any of the dynamic interfaces, or a WLAN to control data traffic to and from wireless clients or to the controller central processing unit (CPU) to control all traffic destined for the CPU.

An access control list (ACL) is a set of rules used to limit access to a particular interface. ACLs are configured on the switch and applied to the management interface and to any of the dynamic interfaces.

You can also create a preauthentication ACL for web authentication. Such an ACL is used to allow certain types of traffic before authentication is complete.

IPv6 ACLs support the same options as IPv4 ACLs including source, destination, source and destination ports.

Note You can enable only IPv4 traffic in your network by blocking IPv6 traffic. That is, you can configure an IPv6 ACL to deny all IPv6 traffic and apply it on specific or all WLANs.

Understanding IPv6 ACLs

A switch supports two types of IPv6 ACLs:

- IPv6 router ACLs are supported on outbound or inbound traffic on Layer 3 interfaces, which can be routed ports, switch virtual interfaces (SVIs), or Layer 3 EtherChannels. IPv6 router ACLs apply only to IPv6 packets that are routed.
- IPv6 port ACLs are supported on inbound traffic on Layer 2 interfaces only. IPv6 port ACLs are applied to all IPv6 packets entering the interface.

A switch running the IP base feature set supports only input router IPv6 ACLs. It does not support port ACLs or output IPv6 router ACLs.

Note If you configure unsupported IPv6 ACLs, an error message appears and the configuration does not take affect.

The switch does not support VLAN ACLs (VLAN maps) for IPv6 traffic.

You can apply both IPv4 and IPv6 ACLs to an interface. As with IPv4 ACLs, IPv6 port ACLs take precedence over router ACLs:

- When an input router ACL and input port ACL exist in an SVI, packets received on ports to which a port ACL is applied are filtered by the port ACL. Routed IP packets received on other ports are filtered by the router ACL. Other packets are not filtered.
- When an output router ACL and input port ACL exist in an SVI, packets received on the ports to which a port ACL is applied are filtered by the port ACL. Outgoing routed IPv6 packets are filtered by the router ACL. Other packets are not filtered.

Note If any port ACL (IPv4, IPv6, or MAC) is applied to an interface, that port ACL is used to filter packets, and any router ACLs attached to the SVI of the port VLAN are ignored.

Related Topics

Creating an IPv6 ACL, on page 97
Applying an IPv6 to an Interface, on page 101
Creating WLAN IPv6 ACL, on page 102
Displaying IPv6 ACLs, on page 103

Types of ACL

Per User IPv6 ACL

For the per-user ACL, the full access control entries (ACE) as the text strings are configured on the ACS.

The ACE is not configured on the Controller. The ACE is sent to the switch in the `ACCESS-Accept` attribute and applies it directly for the client. When a wireless client roams into an foreign switch, the ACEs are sent to the foreign switch as an AAA attribute in the mobility Handoff message. Output direction, using per-user ACL is not supported.

Filter ID IPv6 ACL

For the filter-Id ACL, the full ACEs and the `acl name(filter-id)` is configured on the switch and only the `filter-id` is configured on the ACS.

The `filter-id` is sent to the switch in the ACCESS-Accept attribute, and the switch looks up the filter-id for the ACEs, and then applies the ACEs to the client. When the client L2 roams to the foreign switch, only the filter-id is sent to the foreign switch in the mobility Handoff message. Output filtered ACL, using per-user ACL is not supported. The foreign switch has to configure the filter-id and ACEs beforehand.

Downloadable IPv6 ACL

For the downloadable ACL(dACL), the full ACEs and the `dacl` name are all configured on the ACS only.

Note The controller does not configure any ACL.

The ACS sends the `dacl` name to the switch in its `ACCESS-Accept` attribute, which takes the `dacl` name and sends the `dACL` name back to the ACS, for the ACEs, using the `access-request` attribute.

The ACS responds to the corresponding ACEs of the switch in the `access-accept` attribute. When the wireless client roams to an foreign switch, only the `dacl` name is sent to the foreign switch in the mobility Handoff message. The foreign switch contacts the ACS server with the `dacl` name to retrieve the ACEs.

Configuring IPv6 ACLs

To filter IPv6 traffic, you perform these steps:

Before you begin

Before configuring IPv6 ACLs, you must select one of the dual IPv4 and IPv6 SDM templates.

Procedure

	Command or Action	Purpose
Step 1	Create an IPv6 ACL, and enter IPv6 access list configuration mode.	
Step 2	Configure the IPv6 ACL to block (deny) or pass (permit) traffic.	
Step 3	Apply the IPv6 ACL to the interface where the traffic needs to be filtered.	
Step 4	Apply the IPv6 ACL to an interface. For router ACLs, you must also configure an IPv6 address on the Layer 3 interface to which the ACL is applied.	

Default IPv6 ACL Configuration

There are no IPv6 ACLs configured or applied.

Interaction with Other Features and Switches

- If an IPv6 router ACL is configured to deny a packet, the packet is not routed. A copy of the packet is sent to the Internet Control Message Protocol (ICMP) queue to generate an ICMP unreachable message for the frame.
- If a bridged frame is to be dropped due to a port ACL, the frame is not bridged.
- You can create both IPv4 and IPv6 ACLs on a switch or switch stack, and you can apply both IPv4 and IPv6 ACLs to the same interface. Each ACL must have a unique name; an error message appears if you try to use a name that is already configured.

  You use different commands to create IPv4 and IPv6 ACLs and to attach IPv4 or IPv6 ACLs to the same Layer 2 or Layer 3 interface. If you use the wrong command to attach an ACL (for example, an IPv4 command to attach an IPv6 ACL), you receive an error message.

- You cannot use MAC ACLs to filter IPv6 frames. MAC ACLs can only filter non-IP frames.

- If the hardware memory is full, for any additional configured ACLs, packets are dropped to the CPU, and the ACLs are applied in software. When the hardware is full a message is printed to the console indicating the ACL has been unloaded and the packets will be dropped on the interface.

Note Only packets of the same type as the ACL that could not be added (ipv4, ipv6, MAC) will be dropped on the interface.

How To Configure an IPv6 ACL

Creating an IPv6 ACL

To create an IPv6 ACL, perform this procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 access-list** *acl_name* **Example:** `Switch# ipv6 access-list access-list-name`	Use a name to define an IPv6 access list and enter IPv6 access-list configuration mode.
Step 4	**{deny|permit} protocol** **Example:** `{deny | permit} protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any |host destination-ipv6-address} [operator [port-number]][dscp value] [fragments][log] [log-input] [routing][sequence value] [time-range name]`	Enter deny or permit to specify whether to deny or permit the packet if conditions are matched. These are the conditions: • For protocol, enter the name or number of an Internet protocol: ahp, esp, icmp, ipv6, pcp, stcp, tcp, or udp, or an integer in the range 0 to 255 representing an IPv6 protocol number. • The source-ipv6-prefix/prefix-length or destination-ipv6-prefix/ prefix-length is the source or destination IPv6 network or class of networks for which to set deny

	Command or Action	Purpose
		or permit conditions, specified in hexadecimal and using 16-bit values between colons (see RFC 2373). • Enter any as an abbreviation for the IPv6 prefix ::/0. • For host source-ipv6-address or destination-ipv6-address, enter the source or destination IPv6 host address for which to set deny or permit conditions, specified in hexadecimal using 16-bit values between colons. • (Optional) For operator, specify an operand that compares the source or destination ports of the specified protocol. Operands are lt (less than), gt (greater than), eq (equal), neq (not equal), and range. If the operator follows the source-ipv6-prefix/prefix-length argument, it must match the source port. If the operator follows the destination-ipv6-prefix/prefix-length argument, it must match the destination port. • (Optional) The port-number is a decimal number from 0 to 65535 or the name of a TCP or UDP port. You can use TCP port names only when filtering TCP. You can use UDP port names only when filtering UDP. • (Optional) Enter dscp value to match a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63. • (Optional) Enter fragments to check noninitial fragments. This keyword is visible only if the protocol is ipv6. • (Optional) Enter log to cause an logging message to be sent to the console about the packet that matches the entry. Enter log-input to include the input interface in the log entry. Logging is supported only for router ACLs.

	Command or Action	Purpose
		• (Optional) Enter routing to specify that IPv6 packets be routed. • (Optional) Enter sequence value to specify the sequence number for the access list statement. The acceptable range is from 1 to 4294967295 • (Optional) Enter time-range name to specify the time range that applies to the deny or permit statement.
Step 5	**{deny|permit} tcp** **Example:** `{deny | permit} tcp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any |hostdestination-ipv6-address} [operator [port-number]][ack] [dscp value][established] [fin] [log][log-input] [neq {port |protocol}] [psh] [range{port | protocol}] [rst][routing] [sequence value] [syn] [time-range name][urg]`	(Optional) Define a TCP access list and the access conditions. Enter tcp for Transmission Control Protocol. The parameters are the same as those described in Step 3, with these additional optional parameters: • ack—Acknowledgment bit set. • established—An established connection. A match occurs if the TCP datagram has the ACK or RST bits set. • fin—Finished bit set; no more data from sender. • neq {port | protocol}—Matches only packets that are not on a given port number. • psh—Push function bit set. • range {port | protocol}—Matches only packets in the port number range. • rst—Reset bit set. • syn—Synchronize bit set. • urg—Urgent pointer bit set.
Step 6	**{deny|permit} udp** **Example:** `{deny | permit} udp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address} [operator [port-number]][dscp value] [log][log-input] [neq {port |protocol}] [range {port`	(Optional) Define a UDP access list and the access conditions. Enter udp for the User Datagram Protocol. The UDP parameters are the same as those described for TCP, except that the operator [port]] port number or name must be a UDP port number or name, and the established parameter is not valid for UDP.

	Command or Action	Purpose
	`|protocol}] [routing][sequence value][time-range name]`	
Step 7	**{deny|permit} icmp** **Example:** `{deny | permit} icmp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address} [operator [port-number]][icmp-type [icmp-code] |icmp-message] [dscpvalue] [log] [log-input] [routing] [sequence value][time-range name]`	(Optional) Define an ICMP access list and the access conditions. Enter icmp for Internet Control Message Protocol. The ICMP parameters are the same as those described for most IP protocols in Step 3a, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings: • icmp-type—Enter to filter by ICMP message type, a number from 0 to 255. • icmp-code—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255. • icmp-message—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name. To see a list of ICMP message type names and code names, use the ? key or see command reference for this release.
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 9	**show ipv6 access-list** **Example:** `show ipv6 access-list`	Verify the access list configuration.
Step 10	**copy running-config startup-config** **Example:** `copy running-config startup-config`	(Optional) Save your entries in the configuration file.

Related Topics

Prerequisites for Configuring IPv6 ACL, on page 93
Understanding IPv6 ACLs, on page 94
Applying an IPv6 to an Interface, on page 101
Creating WLAN IPv6 ACL, on page 102
Displaying IPv6 ACLs, on page 103

Applying an IPv6 to an Interface

This section describes how to apply IPv6 ACLs to network interfaces. You can apply an IPv6 ACL to outbound or inbound traffic on layer 2 and Layer 3 interfaces. You can apply IPv6 ACLs only to inbound management traffic on Layer 3 interfaces.

To control access to an interface, perform this procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface_id* **Example:** `Switch# interface interface-id`	Identifies a Layer 2 interface (for port ACLs) or Layer 3 Switch Virtual interface (for router ACLs) on which to apply an access list, and enters interface configuration mode.
Step 4	**no switchport** **Example:** `Switch# no switchport`	Changes the interface from Layer 2 mode (the default) to Layer 3 mode (only if applying a router ACL).
Step 5	**ipv6 address** *ipv6_address* **Example:** `Switch# ipv6 address ipv6-address`	Configures an IPv6 address on a Layer 3 interface (for router ACLs). **Note** This command is not required on Layer 2 interfaces or if the interface has already been configured with an explicit IPv6 address.
Step 6	**ipv6 traffic-filter** *acl_name* **Example:** `Switch# ipv6 traffic-filter access-list-name {in | out}`	Applies the access list to incoming or outgoing traffic on the interface.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 8	**show running-config interface tenGigabitEthernet 1/0/3**	Shows the configuration summary.

	Command or Action	Purpose

	Example:
	`Switch# show running-config interface tenGigabitEthernet 1/0/3`
	`.....`
	`.....`
	`Building configuration .....`
	`.....`
	`Current configuration : 98 bytes`
	`!`
	`interface TenGigabitEthernet1/0/3`
	`switchport mode trunk`
	`ipv6 traffic-filter MyFilter out`
	`end`	

Step 9	**copy running-config startup-config** **Example:** `copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Creating an IPv6 ACL, on page 97
Understanding IPv6 ACLs, on page 94
Creating WLAN IPv6 ACL, on page 102
Displaying IPv6 ACLs, on page 103

Creating WLAN IPv6 ACL

Procedure

	Command or Action	Purpose
Step 1	**ipv6 traffic-filter acl** *acl_name* **Example:** `Switch(config-wlan)# ipv6 traffic-filter acl <acl_name>`	Creates a named WLAN ACL.
Step 2	**ipv6 traffic-filter acl web** **Example:** `Switch(config-wlan)# ipv6 traffic-filter acl web <acl_name-preauth>`	Creates a pre-authentication for WLAN ACL.

```
Switch(config-wlan)# ipv6 traffic-filter acl <acl_name>
Switch(config-wlan)#ipv6 traffic-filter acl web <acl_name-preauth>
```

Related Topics

Creating an IPv6 ACL, on page 97
Applying an IPv6 to an Interface, on page 101
Understanding IPv6 ACLs, on page 94
Displaying IPv6 ACLs, on page 103

Verifying IPv6 ACL

Displaying IPv6 ACLs

To displayIPv6 ACLs, perform this procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**show access-list** **Example:** `Switch# show access-lists`	Displays all access lists configured on the switch
Step 4	**show ipv6 access-list** *acl_name* **Example:** `Switch# show ipv6 access-list [access-list-name]`	Displays all configured IPv6 access list or the access list specified by name.

Related Topics

Creating an IPv6 ACL, on page 97
Applying an IPv6 to an Interface, on page 101
Creating WLAN IPv6 ACL, on page 102
Understanding IPv6 ACLs, on page 94

Configuration Examples for IPv6 ACL

Example: Creating an IPv6 ACL

This example configures the IPv6 access list named CISCO. The first deny entry in the list denies all packets that have a destination TCP port number greater than 5000. The second deny entry denies packets that have a source UDP port number less than 5000. The second deny also logs all matches to the console. The first permit entry in the list permits all ICMP packets. The second permit entry in the list permits all other traffic.

The second permit entry is necessary because an implicit deny -all condition is at the end of each IPv6 access list.

Note Logging is supported only on Layer 3 interfaces.

```
Switch(config)# ipv6 access-list CISCO
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch (config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any
```

Example: Applying IPv6 ACLs

This example shows how to apply the access list Cisco to outbound traffic on a Layer 3 interface.

```
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CISCO out
```

Example: Displaying IPv6 ACLs

This is an example of the output from the **show access-lists** privileged EXEC command. The output shows all access lists that are configured on the switch or switch stack.

```
Switch #show access-lists
Extended IP access list hello
10 permit ip any any
IPv6 access list ipv6
permit ipv6 any any sequence 10
```

This is an example of the output from the show ipv6 access-lists privileged EXEC command. The output shows only IPv6 access lists configured on the switch or switch stack.

```
Switch# show ipv6 access-list
IPv6 access list inbound
permit tcp any any eq bgp (8 matches) sequence 10
permit tcp any any eq telnet (15 matches) sequence 20
permit udp any any sequence 30

IPv6 access list outbound
deny udp any any sequence 10
deny tcp any any eq telnet sequence 20
```

Example: Configuring RA Throttling and NS Suppression

This task describes how to create an RA throttle policy in order to help the power-saving wireless clients from being disturbed by frequent unsolicited periodic RA's. The unsolicited multicast RA is throttled by the controller.

Before you begin

Enable IPv6 on the client machine.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ipv6 nd ra-throttler policy Mythrottle** **Example:** `Switch (config)# ipv6 nd ra-throttler policy Mythrottle`	Creates a RA throttler policy called Mythrottle.
Step 3	**throttle-period 20** **Example:** `Switch (config-nd-ra-throttle)# throttle-period 20`	Determines the time interval segment during which throttling applies.
Step 4	**max-through 5** **Example:** `Switch (config-nd-ra-throttle)# max-through 5`	Determines how many initial RA's are allowed.
Step 5	**allow at-least 3 at-most 5** **Example:** `Switch (config-nd-ra-throttle)# allow at-least 3 at-most 5`	Determines how many RA's are allowed after the initial RAs have been transmitted, until the end of the interval segment.
Step 6	**switch (config)# vlan configuration 100** **Example:** `Switch (config)# vlan configuration 100`	Creates a per vlan configuration.
Step 7	**ipv6 nd suppress** **Example:** `Switch (config)# ipv6 nd suppress`	Disables the neighbor discovery on the Vlan.
Step 8	**ipv6 nd ra-th attach-policy attach-policy_name** **Example:** `Switch (config)# ipv6 nd ra-throttle attach-policy attach-policy_name`	Enables the router advertisement throttling.
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring RA Guard Policy

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 nd raguard policy** *policy name* **Example:** `Switch(config)# ipv6 nd raguard policy MyPolicy`	
Step 4	**trusted-port** **Example:** `Switch(config-nd-raguard)# trusted-port`	Configures the trusted port for the policy created above.

Step 5	**device-role router**
	Example:
	`Switch(config-nd-raguard)# device-role [host|monitor|router|switch]`
	`Switch(config-nd-raguard)# device-role router`
	`d`
		Defines the trusted device that can send RAs to the trusted port created above.

Step 6	**interface** *interface-id* **Example:** `Switch(config)# interface tenGigabitEthernet 1/0/1`	Configures the interface to the trusted device.
Step 7	**ipv6 nd raguard attach-policy** *policy name* **Example:** `Switch(config-if)# ipv6 nd raguard attach-policy Mypolicy`	Configures and attaches the policy to trust the RA's received from the port.
Step 8	**vlan** *vlan-id* **Example:** `Switch(config)# vlan configuration 19-21,23`	Configures the wireless client vlans.
Step 9	**ipv6 nd suppress** **Example:**	Suppresses the ND messages over wireless.

	Command or Action	Purpose
	`Switch(config-vlan-config)# ipv6 nd suppress`	
Step 10	**ipv6 snooping** **Example:** `Switch(config-vlan-config)# ipv6 snooping`	Captures IPv6 traffic.
Step 11	**ipv6 nd raguard attach-policy** *policy name* **Example:** `Switch(config-vlan-config)# ipv6 nd raguard attach-policy Mypolicy`	Attaches the RA Guard policy to the wireless client vlans.
Step 12	**ipv6 nd ra-throttler attach-policy** *policy name* **Example:** `Switch(config-vlan-config)# ipv6 nd ra-throttler attach-policy Mythrottle`	Attaches the RA throttling policy to the wireless client vlans.

Configuring IPv6 Neighbor Binding

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 neighbor binding** [vlan] **19 2001:db8::25:4 interface tenGigabitEthernet 1/0/3 aaa.bbb.ccc** **Example:** `Switch(config)# ipv6 neighbor binding vlan 19 2001:db8::25:4 interface tenGigabitEthernet 1/0/3 aaa.bbb.ccc`	Sets and validates the neighbor 2001:db8::25:4 only valid when transmitting on VLAN 19 through interface te1/0/3 with the source mac-address as aaa.bbb.ccc.

Additional References

Related Documents

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

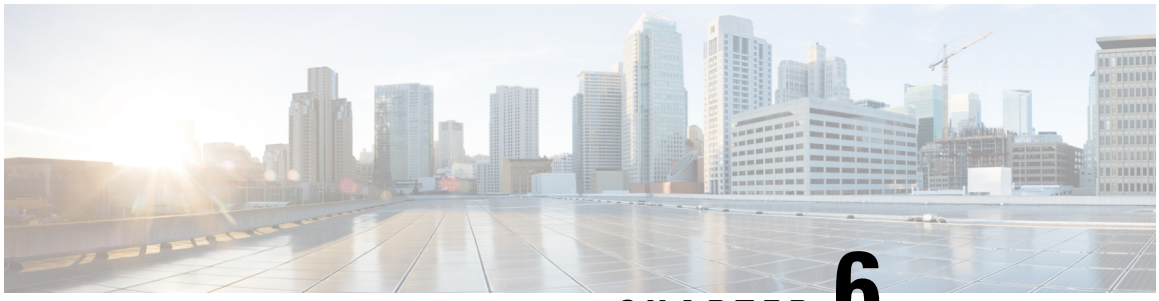
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for IPv6 ACLs

This table lists the features in this module and provides links to specific configuration information:

Feature	Release	Modification
IPv6 ACL Functionality	Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 6

Configuring IPv6 Web Authentication

Prerequisites for IPv6 Web Authentication

The following configurations must be in place before you start with IPv6 Web Authentication:

- IPv6 Device Tracking.
- IPv6 DHCP Snooping.
- Disable security of type 802.1x on the wlan.
- Each WLAN must have a vlan associated to it.
- Change the default wlan setting from **shutdown** to **no shutdown**.

Related Topics

Enabling Security on the WLAN, on page 112

Restrictions for IPv6 Web Authentication

The following restrictions are implied when using IPv6 web authentication:

Related Topics

Enabling Security on the WLAN, on page 112

Information About IPv6 Web Authentication

Web authentication is a Layer 3 security feature and the switch disallows IP traffic (except DHCP and DNS -related packets) from a particular client until it supplies a valid username and password. It is a simple authentication method without the need for a supplicant or client utility. Web authentication is typically used by customers who deploy a guest-access network. Traffic from both, HTTP and HTTPS, page is allowed to display the login page.

Note Web authentication does not provide data encryption and is typically used as simple guest access for either a hot spot or campus atmosphere, where connectivity is always a factor.

A WLAN is configured as **security webauth** for web based authentication. The switch supports the following types of web based authentication:

- Web Authentication – The client enters the credentials in a web page which is then validated by the Wlan controller.
- Web Consent – The Wlan controller presents a policy page with Accept/Deny buttons. Click Accept button to access the network.

A Wlan is typically configured for open authentication, that is without Layer 2 authentication, when web-based authentication mechanism is used.

Web Authentication Process

The following events occur when a WLAN is configured for web authentication:

- The user opens a web browser and enters a URL address, for example, *http://www.example.com*. The client sends out a DNS request for this URL to get the IP address for the destination. The switch bypasses the DNS request to the DNS server, which in turn responds with a DNS reply that contains the IP address of the destination *www.example.com*. This, in turn, is forwarded to the wireless clients.
- The client then tries to open a TCP connection with the destination IP address. It sends out a TCP SYN packet destined to the IP address of *www.example.com*.
- The switch has rules configured for the client and cannot act as a proxy for *www.example.com*. It sends back a TCP SYN-ACK packet to the client with source as the IP address of *www.example.com*. The client sends back a TCP ACK packet in order to complete the three-way TCP handshake and the TCP connection is fully established.
- The client sends an HTTP GET packet destined to *www.example.com*. The switch intercepts this packet and sends it for redirection handling. The HTTP application gateway prepares an HTML body and sends it back as the reply to the HTTP GET requested by the client. This HTML makes the client go to the default web-page of the switch, for example, *http://<Virtual-Server-IP>/login.html*.
- The client closes the TCP connection with the IP address, for example, *www.example.com*.
- If the client wants to go to virtual IP, the client tries to open a TCP connection with the virtual IP address of the switch. It sends a TCP SYN packet for virtual IP to the switch.

- The switch responds back with a TCP SYN-ACK and the client sends back a TCP ACK to the switch in order to complete the handshake.
- The client sends an HTTP GET for */login.html* destined to virtual IP in order to request for the login page.
- This request is allowed to the web server of the switch, and the server responds with the default login page. The client receives the login page in the browser window where the user can log in.

Related Topics

Disabling WPA, on page 111
Enabling Security on the WLAN, on page 112
Enabling a Parameter Map on the WLAN, on page 112
Enabling Authentication List on WLAN, on page 113
Configuring a Global WebAuth WLAN Parameter Map, on page 113
Configuring the WLAN, on page 114
Enabling IPv6 in Global Configuration Mode, on page 115
Verifying the Parameter Map, on page 116
Verifying Authentication List, on page 116

How to Configure IPv6 Web Authentication

Disabling WPA

Before you begin

Disable 802.1x. A typical web authentication does not use Layer 2 security. Use this configuration to remove Layer 2 security.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**wlan test1 2 test1** **Example:** `Switch(config)# wlan test1 2 test1`	Creates a WLAN and assign an SSID to it.
Step 3	**no security** wpa **Example:** `Switch(config-wlan)# no security wpa`	Disables the WPA support for Wlan.

What to do next

Enable the following:

- Security Web Authentication.
- Parameter Local.
- Authentication List.

Related Topics

Web Authentication Process, on page 110

Enabling Security on the WLAN

Procedure

	Command or Action	Purpose
Step 1	**parameter-map type web-auth global** **Example:** `Switch(config)# parameter-map type web-auth global`	Applies the parameter map to all the web-auth wlans.
Step 2	**virtual-ip ipv4 192.0.2.1** **Example:** `Switch(config-params-parameter-map)# virtual-ip ipv4 192.0.2.1`	Defines the virtual gateway IPv4 address.
Step 3	**virtual-ip ipv6 2001:db8::24:2** **Example:** `Switch(config-params-parameter-map)# virtual-ip ipv6 2001:db8::24:2`	Defines the virtual gateway IPv6 address.

Related Topics

Prerequisites for IPv6 Web Authentication, on page 109
Restrictions for IPv6 Web Authentication, on page 109
Web Authentication Process, on page 110

Enabling a Parameter Map on the WLAN

Procedure

	Command or Action	Purpose
Step 1	**security web-auth parameter-map <mapname>** **Example:**	Enables web authentication for the wlan and creates a parameter map.

	Command or Action	Purpose
	`Switch(config-wlan)# security web-auth parameter-map webparalocal`	

Related Topics

Web Authentication Process, on page 110

Enabling Authentication List on WLAN

Procedure

	Command or Action	Purpose
Step 1	**security web-auth authentication-list webauthlistlocal** **Example:** `Switch(config-wlan)# security web-auth`	Enables web authentication for the wlan and creates a local web authentication list.

Related Topics

Web Authentication Process, on page 110

Configuring a Global WebAuth WLAN Parameter Map

Use this example to configure a global web auth WLAN and add a parameter map to it.

Procedure

	Command or Action	Purpose
Step 1	**parameter-map type webauth global** **Example:** `Switch (config)# parameter-map type webauth global`	Configures a global webauth and adds a parameter map to it.
Step 2	**virtual-ip ipv6 2001:db8:4::1** **Example:** `Switch (config-params-parameter-map)# virtual-ip ipv6 2001:db8:4::1`	Defines a virtual gateway IP address that appears to the wireless clients for authentication.
Step 3	**ratelimit init-state-sessions 120** **Example:** `Switch (config-params-parameter-map)# ratelimit init-state-sessions 120`	Sets the global ratelimit to limit the bandwidth that the web clients can use on the switch to avoid over-flooding attacks.

	Command or Action	Purpose
Step 4	**max-https-conns 70** **Example:** `Switch (config-params-parameter-map)# max-http-conns 70`	Sets the maximum number of attempted http connections on the switch to avoid over-flooding atatcks.

Related Topics

Web Authentication Process, on page 110
Configuring the WLAN, on page 114

Configuring the WLAN

Before you begin

- The WLAN must have a Vlan associated with it. By default, a new Wlan is always associated with Vlan 1, which can be changed as per the configuration requirements.
- Configure and enable the WLAN to *no shutdown*. By default, the Wlan is configured with the *shutdown* parameter and is disabled.

Procedure

	Command or Action	Purpose
Step 1	**wlan** *1* **Example:** `Switch(config-wlan)# wlan 1 name vicweb ssid vicweb`	Creates a wlan and assign an SSID to it.
Step 2	**client vlan** *interface ID* **Example:** `Switch(config-wlan)# client vlan VLAN0136`	Assigns the client to vlan interface.
Step 3	**security web-auth authentication list webauthlistlocal** **Example:** `Switch(config-wlan)# security web-auth authentication-list webauthlistlocal`	Configures web authentication for the wlan.
Step 4	**security web-auth parameter-map global** **Example:** `Switch(config-wlan)# security web-auth parameter-map global`	Configures the parameter map on the wlan.
Step 5	**no security wpa** **Example:** `Switch(config-wlan)# no security wpa`	Configures the security policy for a wlan. This enables the wlan.

	Command or Action	Purpose
Step 6	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Configures and enables the Wlan.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Configuring a Global WebAuth WLAN Parameter Map, on page 113
Web Authentication Process, on page 110
Enabling IPv6 in Global Configuration Mode, on page 115

Enabling IPv6 in Global Configuration Mode

Enable IPv6 in global configuration for web authentication.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**web-auth global** **Example:** `Switch(config)# parameter-map type webauth global`	Globally configures the parameter map type as web authentication.
Step 3	**virtual IPv6** **Example:** `Switch(config-params-parameter-map)# virtual-ip ipv6`	Selects IPv6 as the virtaul IP for web authentication. **Note** You can also select IPv4 as the preferred IP for web authentication.

Related Topics

Configuring the WLAN, on page 114
Web Authentication Process, on page 110
Verifying the Parameter Map, on page 116

Verifying IPv6 Web Authentication

Verifying the Parameter Map

Use the **show running configuration** command to verify the parameter map configured for Wlan.

Procedure

	Command or Action	Purpose
Step 1	**show running config** **Example:** `Switchshow running config`	Displays the entire running configuration for the switch. Grep for parameter map to view the result.

```
wlan alpha 2 alpha
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 security web-auth authentication-list webauthlistlocal
 security web-auth parameter-map webparalocal
```

Related Topics

Enabling IPv6 in Global Configuration Mode, on page 115
Web Authentication Process, on page 110
Verifying Authentication List, on page 116

Verifying Authentication List

Use the **show running configuration** command to verify the authentication list configured for the Wlan.

Procedure

	Command or Action	Purpose
Step 1	**show running configuration** **Example:** `Switch#show running-config`	Displays the Wlan configuration. `Switch# show running-config`
Step 2	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

```
Switch#show running-config
 ..................................
 ..................................
 ..................................
 wlan alpha 2 alpha
```

```
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list webauthlistlocal
security web-auth parameter-map webparalocal
.................................
.................................
.................................
```

Related Topics

Verifying the Parameter Map, on page 116
Web Authentication Process, on page 110

Additional References

Related Documents

Related Topic	Document Title
IPv6 command reference	*IPv6 Command Reference (Catalyst 3850 Switches)IPv6 Command Reference (Cisco WLC 5700 Series)*
Web Authentication configuration	*Security Configuration Guide (Catalyst 3850 Switches)Security Configuration Guide (Cisco WLC 5700 Series)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

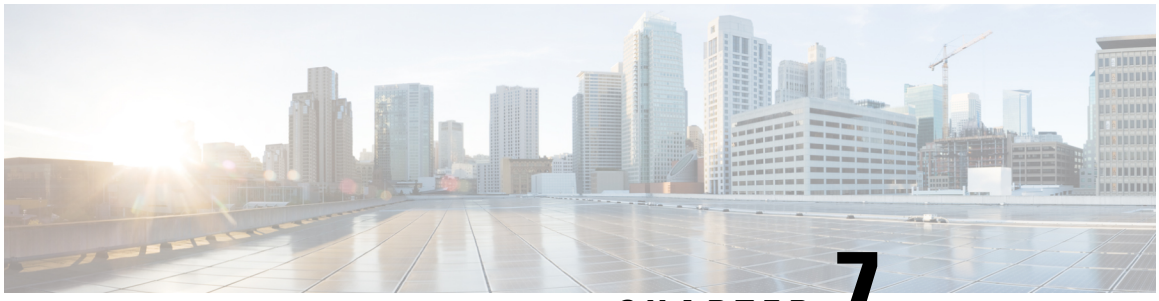
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for IPv6 Web Authentication

This table lists the features in this module and provides links to specific configuration information:

Feature	Release	Modification
IPv6 Web Authentication Functionality	Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 7

Configuring IPv6 Client Mobility

Prerequisites for IPv6 Client Mobility

- To enable wireless IPv6 client connectivity, the underlying wired network must support IPv6 routing and an address assignment mechanism such as SLAAC or DHCPv6. The switch must have L2 adjacency to the IPv6 router, and the VLAN needs to be tagged when the packets enter the switch. APs do not require connectivity on an IPv6 network, as all traffic is encapsulated inside the IPv4 CAPWAP tunnel between the AP and switch.

Restrictions For IPv6 Client Mobility

- When using the IPv6 Client Mobility, clients must support IPv6 with either static stateless auto configuration (such as Windows XP clients) or stateful DHCPv6 IP addressing (such as Windows 7 clients).
- To allow smooth operation of stateful DHCPv6 IP addressing, you must have a switch or router that supports the DHCP for IPv6 feature (such as the switch) that is configured to act like a DHCPv6 server, or you need a dedicated server such as a Windows 2008 server with a built-in DHCPv6 server.

Information About IPv6 Client Mobility

The Switch supports IPv6 mobility for IPv6-only or dual-stack nodes. The IPv6 Client Mobility is divided into:

- Link Layer and

- Network Layer

The link layer is handled by the 802.11 protocol which enables the client to roam to any AP in the same BSS (basic service set) identified by the same SSID without losing the link layer connectivity.

However, link layer mobility is not enough to make wireless client Layer 3 applications continue to work seamlessly while roaming. Cisco IOSd's wireless mobility module uses mobility tunneling to retain seamless connectivity for the client's Layer 3 PoP (point of presence) when the client roams across different subnets on different switches.

IPv6 is the next-generation network layer Internet protocol intended to replace IPv4 in the TCP/IP suite of protocols. This new version increases the internet global address space to accommodate users and applications that require unique global IP addresses. IPv6 incorporates 128-bit source and destination addresses, which provide significantly more addresses than the 32-bit IPv4 addresses.

To support IPv6 clients across controllers, ICMPv6 messages must be dealt with specially to ensure the IPv6 client remains on the same Layer 3 network. The switch keeps track of IPv6 clients by intercepting the ICMPv6 messages to provide seamless mobility and protect the network from network attacks. The NDP (neighbor discovery packets) packets are converted from multicast to unicast and delivered individually per client. This unique solution ensures that Neighbor Discovery and Router Advertisement packets are not leaked across VLANs. Clients can receive specific Neighbor Discovery and Router Advertisement packets ensuring correct IPv6 addressing to avoid unnecessary multicast traffic.

The configuration for IPv6 mobility is the same as IPv4 mobility and requires no separate software on the client side to achieve seamless roaming. The switch must be part of the same mobility group. Both IPv4 and IPv6 client mobility are enabled by default.

IPv6 client mobility is used for the following:

- Retaining the client IPv6 multiple addresses in Layer-2 and Layer-3 roaming.
- IPv6 Neighbor Discovery Prootcol (NDP) packet management.
- Client IPv6 addresses learning.

Note The configuration for IPv6 mobility in SDA wireless and Local mode is the same as of IPv4 mobility and requires no different software configuration on the client side to achieve seamless roaming. Refer to IPv4 mobility section for configuration information.

Using Router Advertisment

The Neighbor Discovery Protocol(NDP) operates in the link-layer and is responsible for the discovery of other nodes on the link. It determines the link-layer addresses of other nodes, finds the available routers, and maintains reachability information about the paths to other active neighbor nodes.

Router Advertisement (RA) is one of the IPv6 Neighbor Discovery Protocol (NDP) packets that is used by the hosts to discover available routers, acquire the network prefix to generate the IPv6 addresses, link MTU, and so on. The routers send RA on a regular basis, or in response to hosts Router Solicitation messages.

IPv6 wireless client mobility manages the IPv6 RA packet . The converged access switch forwards the link-local all-nodes multicast RA packets to the local and roaming wireless nodes mapped on same VLAN the RA was received on.

Figure 1 illustrates the link-local all-nodes mcast RA forwarding issue in the wireless node mobility.

Figure 5: Roaming Client Receiving Invalid RA from Router 2

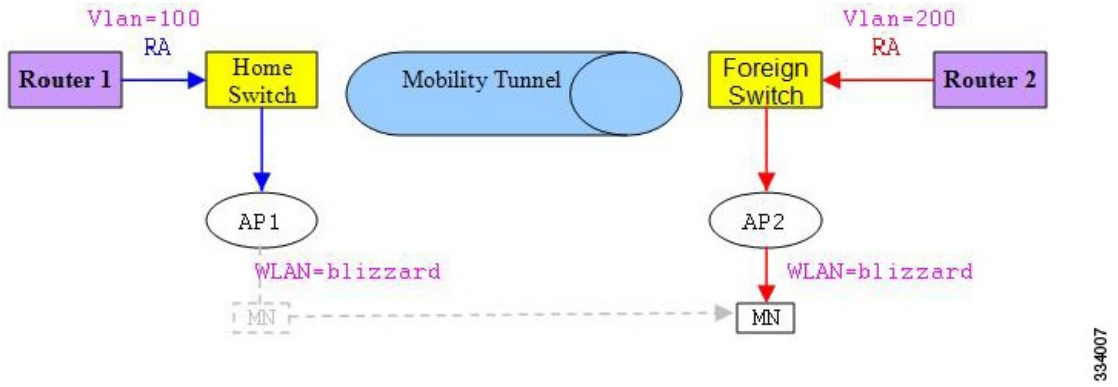
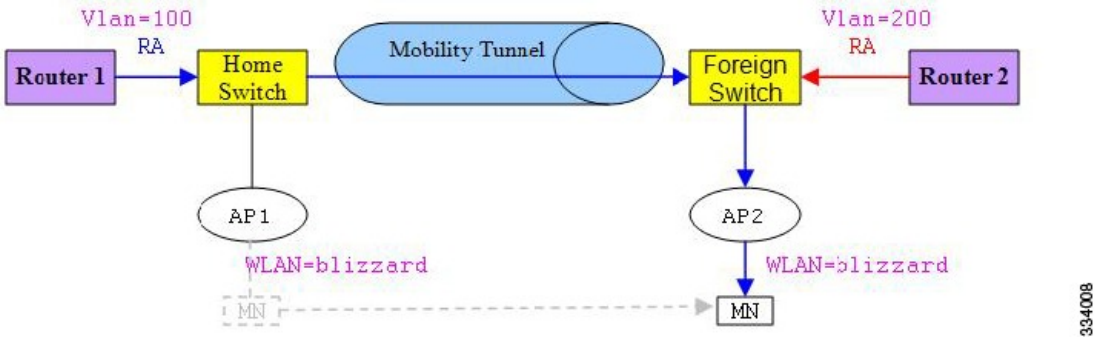


Figure 2 illustrates how a roaming client “MN” receives RA from VLAN 200 in a foreign switch and how it acquires an new IP address and breaks into L3 mobility's point of presence.

Figure 6: Roaming Client Receives Valid RA from Router 1



Related Topics

Verifying IPv6 Client Mobility, on page 122
Monitoring IPv6 Client Mobility, on page 123

RA Throttling and NS suppression

To safeguard the power-saving wireless clients form being disturbed by frequent unsolicited periodic RAs, the controller can throttle the unsolicited multicast RA.

Related Topics

Verifying IPv6 Client Mobility, on page 122
Monitoring IPv6 Client Mobility, on page 123

IPv6 Address Learning

There are three ways for IPv6 client to acquire IPv6 addresses:

- Stateless Address Auto-Configuration (SLAAC)
- Stateful DHCPv6
- Static configuration

For these methods, the IPv6 client always sends NS DAD (duplicate address detection) to ensure that there is no duplicated IP address on the network. The switch snoops the clients NDP and DHCPv6 packets to learn about its client IP addresses and then updates the controllers database. The database then informs the controller for the clients new IP address.

Related Topics

Verifying IPv6 Client Mobility, on page 122
Monitoring IPv6 Client Mobility, on page 123

Handling Multiple IP Addresses

In the case when the new IP address is received after RUN state, whether an addition or removal, the controller updates the new IP addresses on its local database for display purposes. Essentially, the IPv6 uses the existing or same PEM state machine code flow as in IPv4. When the IP addresses are requested by external entities, for example, from Prime Infrastructure, the controller will include all the available IP addresses, IPv4 and IPv6, in the API/SPI interface to the external entities.

An IPv6 client can acquire multiple IP addresses from stack for different purposes. For example, a link-local address for link local traffic, and a routable unique local or global address.

When the client is in the DHCP request state and the controller receives the first IP address notification from the database for either an IPv4 or IPv6 address, the PEM moves the client into the RUN state.

When a new IP address is received after the RUN state, either for addition or removal, the controller updates the new IP addresses on its local database for display purposes.

When the IP addresses are requested by external entities, for example, from Prime Infrastructure, the controller provides the available IP addresses, both IPv4 and IPv6, to the external entities.

Related Topics

Verifying IPv6 Client Mobility, on page 122
Monitoring IPv6 Client Mobility, on page 123

IPv6 Configuration

The switch supports IPv6 client as seamlessly as the IPv4 clients. The administrator must manually configure the VLANs to enable the IPv6, IPv6's snooping and throttling functionality. This will enable the NDP packets to throttle between the switch and its various clients.

Related Topics

Verifying IPv6 Client Mobility, on page 122
Monitoring IPv6 Client Mobility, on page 123

Verifying IPv6 Client Mobility

The commands listed in the Table 1 applies to the IPv6 client mobility.

Table 4: Commands for Verifying IPv6 Client Mobility on Cisco 5760 WLC

Command	Description
debug mobility ipv6	Enables all the wireless client IPv6 mobility debugs.
debug **client** **mac-address** **(mac-addr)**	Displays wireless client debugging. Enter a MAC address for debugging information.

Related Topics

Using Router Advertisment, on page 120
RA Throttling and NS suppression, on page 121
IPv6 Address Learning, on page 121
Handling Multiple IP Addresses, on page 122
IPv6 Configuration, on page 122
Monitoring IPv6 Client Mobility, on page 123

Monitoring IPv6 Client Mobility

The commands in Table 2 are used to monitor IPv6 Client mobility on the switch.

Table 5: Monitoring IPv6 Client Mobility Commands

Commands	Description
show wireless client summary	Displays the wireless specific configuration of active clients.
show wireless client mac-address **(mac-addr)**	Displays the wireless specific configuration of active clients based on their MAC address.

Related Topics

Verifying IPv6 Client Mobility, on page 122
Using Router Advertisment, on page 120
RA Throttling and NS suppression, on page 121
IPv6 Address Learning, on page 121
Handling Multiple IP Addresses, on page 122
IPv6 Configuration, on page 122

Additional References

Related Documents

Related Topic	Document Title
IPv6 command reference	*IPv6 Command Reference (Catalyst 3850 Switches)IPv6 Command Reference (Cisco WLC 5700 Series)*
Mobility configuration	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

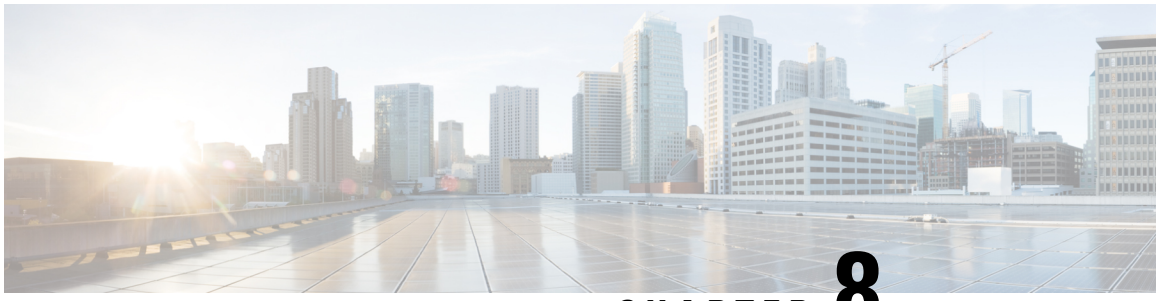
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for IPv6 Client Mobility

This table lists the features in this module and provides links to specific configuration information:

Feature	Release	Modification
IPv6 Client Mobility Functionality	Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 8

Configuring IPv6 Mobility

Pre-requisites for IPv6 Mobility

The mobility and its related infrastructure must be configured and ready for use.

Information About IPv6 Mobility

Mobility, or roaming, is a wireless LAN client's ability to maintain its association seamlessly from one access point to another securely and with as little latency as possible. This section explains how mobility works whenswitch are included in a wireless network.

When a wireless client associates and authenticates to an access point, the access point's switch places an entry for that client in its client database. This entry includes the client's MAC and IP addresses, security context and associations, quality of service (QoS) contexts, the WLAN, and the associated access point. The switch uses this information to forward frames and manage traffic to and from the wireless client.

When the wireless client moves its association from one access point to another, the switch simply updates the client database with the newly associated access point. If necessary, new security context and associations are established as well. The process becomes more complicated, however, when a client roams from an access point joined to one switch to an access point joined to a different switch. It also varies based on whether theswitch are operating on the same subnet.

Inter Controller Roaming

When the client associates to an access point joined to a new switch, the new switch exchanges mobility messages with the original switch, and the client database entry is moved to the new switch if sticky anchoring is disabled.

Related Topics

Monitoring IPv6 Mobility, on page 128

Intra Subnet Roaming with Sticky Anchoring, and Inter Subnet Roaming

Inter-subnet roaming is similar to inter-controller roaming in that the switch exchange mobility messages on the client roam. However, instead of moving the client database entry to the new switch, the original switch marks the client with an "Anchor" entry in its own client database. The database entry is copied to the new switch client database and marked with a "Foreign" entry in the new switch. The roam remains transparent to the wireless client, and the client maintains its original IP address.

In inter-subnet roaming, WLANs on both anchor and foreign switch need to have the same network access privileges and no source-based routing or source-based firewalls in place. Otherwise, the clients may have network connectivity issues after the handoff.

For more information on configuring mobility see, the Cisco 5700 Wireless LAN Controller Mobility Configuration Guide, Cisco IOS XE, Release 3.2SE.

Related Topics

Monitoring IPv6 Mobility, on page 128

How to Configure IPv6 Mobility

Monitoring IPv6 Mobility

This chapter displays the mobility related IPv6 configuration. To see the mobility related configurations refer to the Cisco 5700 Wireless LAN Controller Mobility Configuration Guide, Cisco IOS XE 3.2SE.

Procedure

	Command or Action	Purpose
Step 1	**show ipv6 neighbors binding mac C0C1.C06B.C4E2** **Example:** `Switch# show ipv6 neighbors binding mac C0C1.C06B.C4E2`	Displays the IPv6 related mobility configurations.

Example

```
Switch# show ipv6 neighbors binding mac C0C1.C06B.C4E2
Binding Table has 45 entries, 37 dynamic (limit 100)
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DHCP, PKT - Other Packet, API
- API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned
```

```
    IPv6 address                              Link-Layer addr Interface vlan prlvl  age
state    Time left
L   FE80:20:25::16                            2037.064C.BA71  Vl25        25  0100 3137mn
REACHABLE
L   FE80:20:24::16                            2037.064C.BA41  Vl24        24  0100 3137mn
REACHABLE
L   FE80:20:23::16                            2037.064C.BA44  Vl23        23  0100 3137mn
REACHABLE
ND  FE80:20:23::13                            2037.0653.6BC4  Te1/0/1     23  0005   85s
REACHABLE  223 s try 0
ND  FE80:20:22::17                            2037.064D.06F6  Te1/0/1     22  0005    3mn
REACHABLE  92 s try 0
L   FE80:20:22::16                            2037.064C.BA76  Vl22        22  0100 3137mn
REACHABLE
ND  FE80:20:22::13                            2037.0653.6BF6  Te1/0/1     22  0005  165s
REACHABLE  136 s try 0
ND  FE80:20:22::12                            2037.064C.94F6  Te1/0/1     22  0005   23s
REACHABLE  281 s try 0
ND  FE80:20:22::2                             0022.550E.8FC3  Te1/0/1     22  0005   18s
REACHABLE  295 s try 0
ND  FE80:20:21::17                            2037.064D.06E8  Te1/0/1     21  0005    4mn
REACHABLE  60 s try 0
L   FE80:20:21::16                            2037.064C.BA68  Vl21        21  0100 3137mn
REACHABLE
ND  FE80:20:21::13                            2037.0653.6BE8  Te1/0/1     21  0005   57s
REACHABLE  252 s try 0
ND  FE80:20:21::12                            2037.064C.94E8  Te1/0/1     21  0005    4s
REACHABLE  297 s
ND  FE80:20:21::2                             0022.550E.8FC2  Te1/0/1     21  0005    2s
REACHABLE  307 s try 0
ND  FE80::F866:8BE0:12E4:39CF                 C0C1.C06B.C4E2  Ca4         21  0005    3mn
REACHABLE  89 s try 0
ND  FE80::6D0A:DB33:D69E:91C7                 0050.B606.A6CE  Te1/0/1     22  0005  135s
REACHABLE  171 s try 0
ND  FE80::985:8189:9937:BB05                  8CA9.8295.09CC  Ca0         21  0005   15s
REACHABLE  287 s
ND  FE80::20:24:13                            2037.0653.6BC1  Te1/0/1     24  0005  155s
REACHABLE  145 s try 0
L   2001:20:23::16                            2037.064C.BA44  Vl23        23  0100 3137mn
REACHABLE
DH  2001:20:22:0:C96C:AF29:5DDC:2689          0050.B606.A6CE  Te1/0/1     22  0024   19s
REACHABLE  286 s try 0(16574
DH  2001:20:22:0:A46B:90B2:F0DB:F952          0050.B606.A6CE  Te1/0/1     22  0024 2339mn
STALE      32401 s
DH  2001:20:22:0:7DFD:14EC:B1E4:1172          0050.B606.A6CE  Te1/0/1     22  0024 2339mn
STALE      24394 s
DH  2001:20:22:0:7CB3:D6DD:FD6A:50F           0050.B606.A6CE  Te1/0/1     22  0024 2333mn
STALE      29195 s
DH  2001:20:22:0:6D32:AF24:FDE1:2504          0050.B606.A6CE  Te1/0/1     22  0024  509mn
STALE      118821 s
DH  2001:20:22:0:5106:5AD:FE98:A2F0           0050.B606.A6CE  Te1/0/1     22  0024 2328mn
STALE      31362 s
ND  2001:20:22::201:13                        0050.B606.A6CE  Te1/0/1     22  0005   49s
REACHABLE  264 s try 0
L   2001:20:22::16                            2037.064C.BA76  Vl22        22  0100 3137mn
REACHABLE
ND  2001:20:22::13                            2037.0653.6BF6  Te1/0/1     22  0005  175s
REACHABLE  131 s try 0
ND  2001:20:22::2                             0022.550E.8FC3  Te1/0/1     22  0005   28s
REACHABLE  274 s try 0
ND  2001:20:21:0:F866:8BE0:12E4:39CF          C0C1.C06B.C4E2  Ca4         21  0005    4mn
REACHABLE  21 s try 0
ND  2001:20:21:0:C085:9D4C:4521:B777          0021.CC73.AA17  Te1/0/1     21  0005   11s
REACHABLE  290 s try 0
```

```
ND  2001:20:21:0:6233:4BFF:FE1A:744C        6033.4B1A.744C  Ca4         21  0005    3mn
REACHABLE  108 s try 0
ND  2001:20:21:0:447E:745D:2F48:1C68        8CA9.8295.09CC  Ca0         21  0005   34s
REACHABLE  276 s
ND  2001:20:21:0:3920:DDE8:B29:AD51         C0C1.C06B.C4E2  Ca4         21  0005    3mn
REACHABLE  87 s try 0
ND  2001:20:21:0:1016:A333:FAD5:6E66        0021.CC73.AA17  Te1/0/1     21  0005    4mn
REACHABLE  18 s try 0
ND  2001:20:21:0:C42:E317:BA9B:EB17         6033.4B1A.744C  Ca4         21  0005    4mn
REACHABLE  61 s try 0
ND  2001:20:21:0:985:8189:9937:BB05         8CA9.8295.09CC  Ca0         21  0005  135s
REACHABLE  173 s try 0
ND  2001:20:21::201:20                      0021.CC73.AA17  Te1/0/1     21  0005    4mn
REACHABLE  43 s try 0
ND  2001:20:21::17                          2037.064D.06E8  Te1/0/1     21  0005    4mn
REACHABLE  50 s try 0
L   2001:20:21::16                          2037.064C.BA68  Vl21        21  0100 3137mn
REACHABLE
ND  2001:20:21::13                          2037.0653.6BE8  Te1/0/1     21  0005   67s
REACHABLE  237 s try 0
ND  2001:20:21::12                          2037.064C.94E8  Te1/0/1     21  0005    5mn
REACHABLE  512 ms try 0
ND  2001:20:21::2                           0022.550E.8FC2  Te1/0/1     21  0005   12s
REACHABLE  294 s try 0
```

Related Topics

Inter Controller Roaming, on page 127
Intra Subnet Roaming with Sticky Anchoring, and Inter Subnet Roaming, on page 128

Additional References

Related Documents

Related Topic	Document Title
IPv6 command reference	*IPv6 Command Reference (Catalyst 3850 Switches)IPv6 Command Reference (Cisco WLC 5700 Series)*
Mobility configurations	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

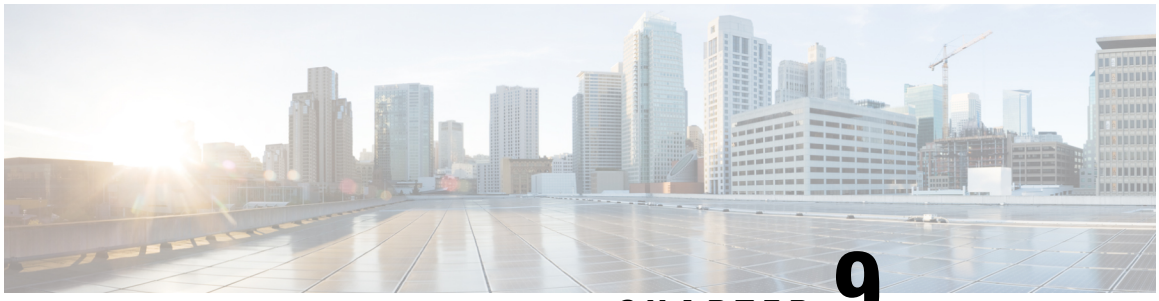
Feature Information for IPv6 Mobility

This table lists the features in this module and provides links to specific configuration information:

Feature	Release	Modification
IPv6 Mobility Functionality	Cisco IOS XE 3.2SE	This feature was introduced.

PART IV

Layer 2/3



CHAPTER 9

Configuring EtherChannels

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for EtherChannels

The following are restrictions for EtherChannels:

- All ports in an EtherChannel must be assigned to the same VLAN or they must be configured as trunk ports.
- Layer 3 EtherChannels are not supported if running the LAN Base license feature set.
- You cannot have a switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches.

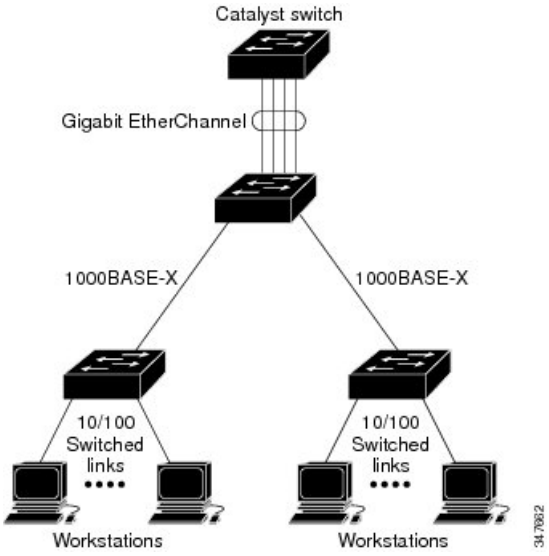
Information About EtherChannels

EtherChannel Overview

EtherChannel provides fault-tolerant high-speed links between switches, routers, and servers. You can use the EtherChannel to increase the bandwidth between the wiring closets and the data center, and you can deploy it anywhere in the network where bottlenecks are likely to occur. EtherChannel provides automatic recovery for the loss of a link by redistributing the load across the remaining links. If a link fails, EtherChannel redirects traffic from the failed link to the remaining links in the channel without intervention.

An EtherChannel consists of individual Ethernet links bundled into a single logical link.

Figure 7: Typical EtherChannel Configuration



Each EtherChannel can consist of up to eight compatibly configured Ethernet ports.

The number of EtherChannels is limited to 128.

All ports in each EtherChannel must be configured as either Layer 2 or Layer 3 ports. The EtherChannel Layer 3 ports are made up of routed ports. Routed ports are physical ports configured to be in Layer 3 mode by using the **no switchport** interface configuration command. For more information, see the Configuring Interface Characteristics chapter.

Related Topics

Configuring Layer 2 EtherChannels (CLI), on page 153
EtherChannel Configuration Guidelines, on page 149
Default EtherChannel Configuration, on page 148
Layer 2 EtherChannel Configuration Guidelines, on page 150

EtherChannel Modes

You can configure an EtherChannel in one of these modes: Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), or On. Configure both ends of the EtherChannel in the same mode:

- When you configure one end of an EtherChannel in either PAgP or LACP mode, the system negotiates with the other end of the channel to determine which ports should become active. If the remote port cannot negotiate an EtherChannel, the local port is put into an independent state and continues to carry data traffic as would any other single link. The port configuration does not change, but the port does not participate in the EtherChannel.
- When you configure an EtherChannel in the **on** mode, no negotiations take place. The switch forces all compatible ports to become active in the EtherChannel. The other end of the channel (on the other switch) must also be configured in the **on** mode; otherwise, packet loss can occur.

Related Topics

Configuring Layer 2 EtherChannels (CLI), on page 153
EtherChannel Configuration Guidelines, on page 149
Default EtherChannel Configuration, on page 148
Layer 2 EtherChannel Configuration Guidelines, on page 150

EtherChannel on Switches

You can create an EtherChannel on a switch, on a single switch in the stack, or on multiple switches in the stack (known as cross-stack EtherChannel).

Figure 8: Single-Switch EtherChannel

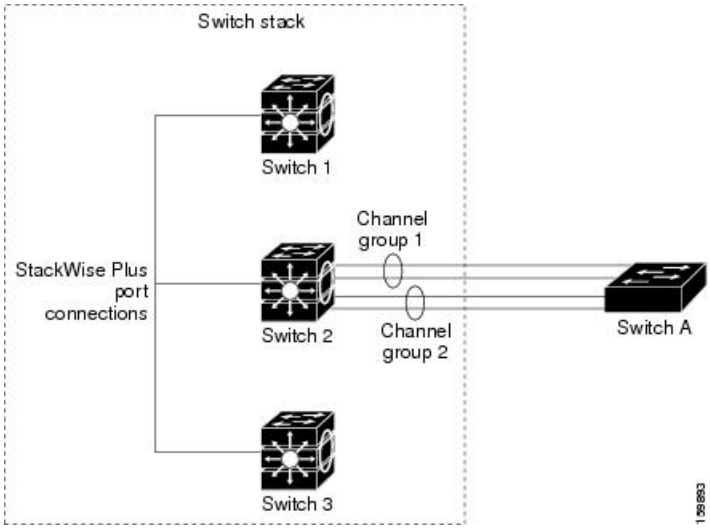


Figure 9: Cross-Stack EtherChannel

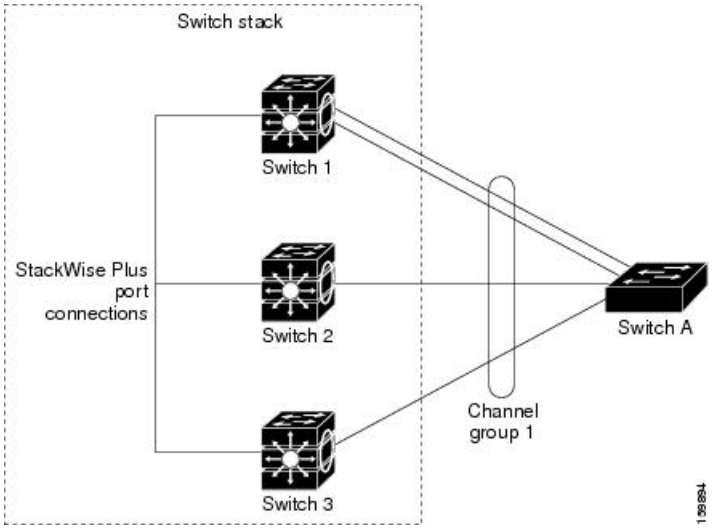
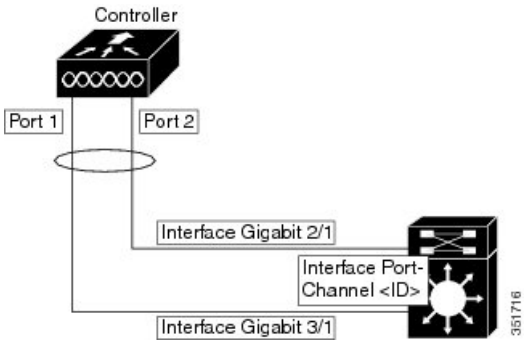
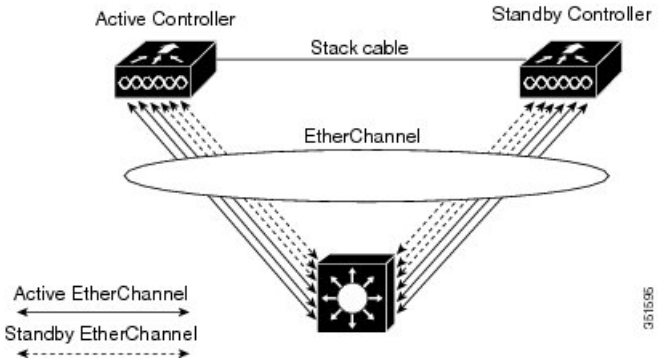


Figure 10: Single Controller EtherChannel



This figure shows the recommended cross-stack EtherChannel configuration with three active links and three standby links.

Figure 11: Cross-Stack EtherChannel



Related Topics

Configuring Layer 2 EtherChannels (CLI), on page 153
EtherChannel Configuration Guidelines, on page 149

Default EtherChannel Configuration, on page 148
Layer 2 EtherChannel Configuration Guidelines, on page 150

EtherChannel Link Failover

If a link within an EtherChannel fails, traffic previously carried over that failed link moves to the remaining links within the EtherChannel. If traps are enabled on the switch, a trap is sent for a failure that identifies the switch, the EtherChannel, and the failed link. Inbound broadcast and multicast packets on one link in an EtherChannel are blocked from returning on any other link of the EtherChannel.

Related Topics

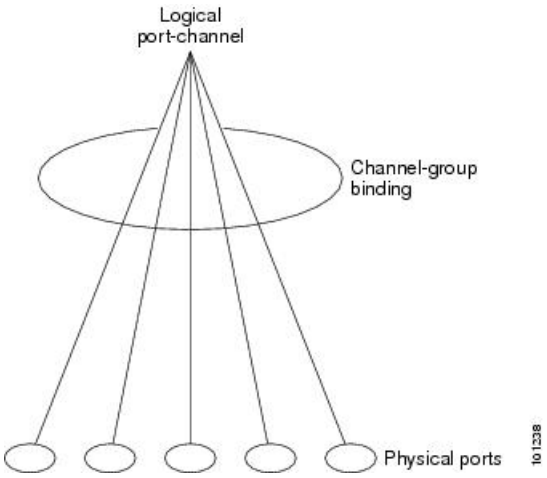
Configuring Layer 2 EtherChannels (CLI), on page 153
EtherChannel Configuration Guidelines, on page 149
Default EtherChannel Configuration, on page 148
Layer 2 EtherChannel Configuration Guidelines, on page 150

Channel Groups and Port-Channel Interfaces

An EtherChannel comprises a channel group and a port-channel interface. The channel group binds physical ports to the port-channel interface. Configuration changes applied to the port-channel interface apply to all the physical ports bound together in the channel group.

Figure 12: Relationship of Physical Ports, Channel Group and Port-Channel Interface

The **channel-group** command binds the physical port and the port-channel interface together. Each EtherChannel has a port-channel logical interface numbered from 1 to 128. This port-channel interface number corresponds to the one specified with the **channel-group** interface configuration command.



- With Layer 2 ports, use the **channel-group** interface configuration command to dynamically create the port-channel interface.

  You also can use the **interface port-channel** *port-channel-number* global configuration command to manually create the port-channel interface, but then you must use the **channel-group** *channel-group-number* command to bind the logical interface to a physical port. The *channel-group-number* can be the same as the *port-channel-number,* or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

- With Layer 3 ports, you should manually create the logical interface by using the **interface port-channel** global configuration command followed by the **no switchport** interface configuration command. You then manually assign an interface to the EtherChannel by using the **channel-group** interface configuration command.
- With Layer 3 ports, use the **no switchport** interface command to configure the interface as a Layer 3 interface, and then use the **channel-group** interface configuration command to dynamically create the port-channel interface.

Related Topics

Creating Port-Channel Logical Interfaces (CLI)
EtherChannel Configuration Guidelines, on page 149
Default EtherChannel Configuration, on page 148
Layer 2 EtherChannel Configuration Guidelines, on page 150
Configuring the Physical Interfaces (CLI)

Port Aggregation Protocol

The Port Aggregation Protocol (PAgP) is a Cisco-proprietary protocol that can be run only on Cisco switches and on those switches licensed by vendors to support PAgP. PAgP facilitates the automatic creation of EtherChannels by exchanging PAgP packets between Ethernet ports. PAgP can be enabled on cross-stack EtherChannels.

By using PAgP, the switch or switch stack learns the identity of partners capable of supporting PAgP and the capabilities of each port. It then dynamically groups similarly configured ports (on a single switch in the stack) into a single logical link (channel or aggregate port). Similarly configured ports are grouped based on hardware, administrative, and port parameter constraints. For example, PAgP groups the ports with the same speed, duplex mode, native VLAN, VLAN range, and trunking status and type. After grouping the links into an EtherChannel, PAgP adds the group to the spanning tree as a single switch port.

PAgP Modes

PAgP modes specify whether a port can send PAgP packets, which start PAgP negotiations, or only respond to PAgP packets received.

Table 6: EtherChannel PAgP Modes

Mode	Description
auto	Places a port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. This setting minimizes the transmission of PAgP packets.
desirable	Places a port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets. This mode is supported when the EtherChannel members are from different switches in the switch stack (cross-stack EtherChannel).

Switch ports exchange PAgP packets only with partner ports configured in the **auto** or **desirable** modes. Ports configured in the **on** mode do not exchange PAgP packets.

Both the **auto** and **desirable** modes enable ports to negotiate with partner ports to form an EtherChannel based on criteria such as port speed. and for Layer 2 EtherChannels, based on trunk state and VLAN numbers.

Ports can form an EtherChannel when they are in different PAgP modes as long as the modes are compatible. For example:

- A port in the **desirable** mode can form an EtherChannel with another port that is in the **desirable** or **auto** mode.
- A port in the **auto** mode can form an EtherChannel with another port in the **desirable** mode.

A port in the **auto** mode cannot form an EtherChannel with another port that is also in the **auto** mode because neither port starts PAgP negotiation.

Related Topics

Configuring Layer 2 EtherChannels (CLI), on page 153
EtherChannel Configuration Guidelines, on page 149
Default EtherChannel Configuration, on page 148
Layer 2 EtherChannel Configuration Guidelines, on page 150
Creating Port-Channel Logical Interfaces (CLI)
Configuring the Physical Interfaces (CLI)

Silent Mode

If your switch is connected to a partner that is PAgP-capable, you can configure the switch port for nonsilent operation by using the **non-silent** keyword. If you do not specify **non-silent** with the **auto** or **desirable** mode, silent mode is assumed.

Use the silent mode when the switch is connected to a device that is not PAgP-capable and seldom, if ever, sends packets. An example of a silent partner is a file server or a packet analyzer that is not generating traffic. In this case, running PAgP on a physical port connected to a silent partner prevents that switch port from ever becoming operational. However, the silent setting allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission.

Related Topics

Configuring Layer 2 EtherChannels (CLI), on page 153
EtherChannel Configuration Guidelines, on page 149
Default EtherChannel Configuration, on page 148
Layer 2 EtherChannel Configuration Guidelines, on page 150
Creating Port-Channel Logical Interfaces (CLI)
Configuring the Physical Interfaces (CLI)

PAgP Learn Method and Priority

Network devices are classified as PAgP physical learners or aggregate-port learners. A device is a physical learner if it learns addresses by physical ports and directs transmissions based on that knowledge. A device is an aggregate-port learner if it learns addresses by aggregate (logical) ports. The learn method must be configured the same at both ends of the link.

When a device and its partner are both aggregate-port learners, they learn the address on the logical port-channel. The device sends packets to the source by using any of the ports in the EtherChannel. With aggregate-port learning, it is not important on which physical port the packet arrives.

PAgP cannot automatically detect when the partner device is a physical learner and when the local device is an aggregate-port learner. Therefore, you must manually set the learning method on the local device to learn

addresses by physical ports. You also must set the load-distribution method to source-based distribution, so that any given source MAC address is always sent on the same physical port.

You also can configure a single port within the group for all transmissions and use other ports for hot-standby. The unused ports in the group can be swapped into operation in just a few seconds if the selected single port loses hardware-signal detection. You can configure which port is always selected for packet transmission by changing its priority with the **pagp port-priority** interface configuration command. The higher the priority, the more likely that the port will be selected.

Note The switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the CLI. The **pagp learn-method** command and the **pagp port-priority** command have no effect on the switch hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports, such as the Catalyst 1900 switch.

When the link partner of the switch is a physical learner, we recommend that you configure the switch as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command. Set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. The switch then sends packets to the physcial learner using the same port in the EtherChannel from which it learned the source address. Only use the **pagp learn-method** command in this situation.

Related Topics

Configuring the PAgP Learn Method and Priority (CLI), on page 160
EtherChannel Configuration Guidelines, on page 149
Default EtherChannel Configuration, on page 148
Monitoring EtherChannel, PAgP, and LACP Status, on page 169
Layer 2 EtherChannel Configuration Guidelines, on page 150

PAgP Interaction with Other Features

The Dynamic Trunking Protocol (DTP) and the Cisco Discovery Protocol (CDP) send and receive packets over the physical ports in the EtherChannel. Trunk ports send and receive PAgP protocol data units (PDUs) on the lowest numbered VLAN.

In Layer 2 EtherChannels, the first port in the channel that comes up provides its MAC address to the EtherChannel. If this port is removed from the bundle, one of the remaining ports in the bundle provides its MAC address to the EtherChannel. For Layer 3 EtherChannels, the MAC address is allocated by the active switch as soon as the interface is created (through the **interface port-channel** global configuration command).

PAgP sends and receives PAgP PDUs only from ports that are up and have PAgP enabled for the auto or desirable mode.

Link Aggregation Control Protocol

The LACP is defined in IEEE 802.3ad and enables Cisco switches to manage Ethernet channels between switches that conform to the IEEE 802.3ad protocol. LACP facilitates the automatic creation of EtherChannels by exchanging LACP packets between Ethernet ports.

By using LACP, the switch or switch stack learns the identity of partners capable of supporting LACP and the capabilities of each port. It then dynamically groups similarly configured ports into a single logical link (channel or aggregate port). Similarly configured ports are grouped based on hardware, administrative, and

port parameter constraints. For example, LACP groups the ports with the same speed, duplex mode, native VLAN, VLAN range, and trunking status and type. After grouping the links into an EtherChannel, LACP adds the group to the spanning tree as a single switch port.

The independent mode behavior of ports in a port channel is changed. With CSCtn96950, by default, standalone mode is enabled. When no response is received from an LACP peer, ports in the port channel are moved to suspended state.

LACP Modes

LACP modes specify whether a port can send LACP packets or only receive LACP packets.

Table 7: EtherChannel LACP Modes

Mode	Description
active	Places a port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.
passive	Places a port into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation. This setting minimizes the transmission of LACP packets.

Both the **active** and **passive LACP** modes enable ports to negotiate with partner ports to an EtherChannel based on criteria such as port speed, and for Layer 2 EtherChannels, based on trunk state and VLAN numbers.

Ports can form an EtherChannel when they are in different LACP modes as long as the modes are compatible. For example:

- A port in the **active** mode can form an EtherChannel with another port that is in the **active** or **passive** mode.
- A port in the **passive** mode cannot form an EtherChannel with another port that is also in the **passive** mode because neither port starts LACP negotiation.

Related Topics

Configuring Layer 2 EtherChannels (CLI), on page 153
EtherChannel Configuration Guidelines, on page 149
Default EtherChannel Configuration, on page 148
Layer 2 EtherChannel Configuration Guidelines, on page 150

LACP and Link Redundancy

LACP port-channel operation, bandwidth availability, and link redundancy can be further refined with the LACP port-channel min-links and the LACP max-bundle features.

The LACP port-channel min-links feature:

- Configures the minimum number of ports that must be linked up and bundled in the LACP port channel.
- Prevents a low-bandwidth LACP port channel from becoming active.
- Causes an LACP port channel to become inactive if there are too few active members ports to supply the required minimum bandwidth.

The LACP max-bundle feature:

- Defines an upper limit on the number of bundled ports in an LACP port channel.
- Allows hot-standby ports with fewer bundled ports. For example, in an LACP port channel with five ports, you can specify a max-bundle of three, and the two remaining ports are designated as hot-standby ports.

Related Topics

Configuring the LACP Max Bundle Feature (CLI), on page 162
Configuring LACP Hot-Standby Ports: Example, on page 172
Configuring the LACP Port Channel Min-Links Feature (CLI), on page 163

LACP Interaction with Other Features

The DTP and the CDP send and receive packets over the physical ports in the EtherChannel. Trunk ports send and receive LACP PDUs on the lowest numbered VLAN.

In Layer 2 EtherChannels, the first port in the channel that comes up provides its MAC address to the EtherChannel. If this port is removed from the bundle, one of the remaining ports in the bundle provides its MAC address to the EtherChannel. For Layer 3 EtherChannels, the MAC address is allocated by the active switch as soon as the interface is created through the **interface port-channel** global configuration command.

LACP sends and receives LACP PDUs only from ports that are up and have LACP enabled for the active or passive mode.

EtherChannel On Mode

EtherChannel **on** mode can be used to manually configure an EtherChannel. The **on** mode forces a port to join an EtherChannel without negotiations. The **on** mode can be useful if the remote device does not support PAgP or LACP. In the **on** mode, a usable EtherChannel exists only when the switches at both ends of the link are configured in the **on** mode.

Ports that are configured in the **on** mode in the same channel group must have compatible port characteristics, such as speed and duplex. Ports that are not compatible are suspended, even though they are configured in the **on** mode.

Caution You should use care when using the **on** mode. This is a manual configuration, and ports on both ends of the EtherChannel must have the same configuration. If the group is misconfigured, packet loss or spanning-tree loops can occur.

Load-Balancing and Forwarding Methods

EtherChannel balances the traffic load across the links in a channel by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the channel. You can specify one of several different load-balancing modes, including load distribution based on MAC addresses, IP addresses, source addresses, destination addresses, or both source and destination addresses. The selected mode applies to all EtherChannels configured on the switch.

Note Layer 3 Equal-cost multi path (ECMP) load balancing is based on source IP address, destination IP address, source port, destination port, and layer 4 protocol. Fragmented packets will be treated on two different links based on the algorithm calculated using these parameters. Any changes in one of these parameters will result in load balancing.

You configure the load-balancing and forwarding method by using the **port-channel load-balance** and the **port-channel load-balance extended**global configuration commands.

Related Topics

Configuring EtherChannel Load-Balancing (CLI), on page 157
EtherChannel Configuration Guidelines, on page 149
Layer 2 EtherChannel Configuration Guidelines, on page 150
Default EtherChannel Configuration, on page 148
Layer 3 EtherChannel Configuration Guidelines, on page 151

MAC Address Forwarding

With source-MAC address forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on the source-MAC address of the incoming packet. Therefore, to provide load-balancing, packets from different hosts use different ports in the channel, but packets from the same host use the same port in the channel.

With destination-MAC address forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on the destination host's MAC address of the incoming packet. Therefore, packets to the same destination are forwarded over the same port, and packets to a different destination are sent on a different port in the channel.

With source-and-destination MAC address forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on both the source and destination MAC addresses. This forwarding method, a combination source-MAC and destination-MAC address forwarding methods of load distribution, can be used if it is not clear whether source-MAC or destination-MAC address forwarding is better suited on a particular switch. With source-and-destination MAC-address forwarding, packets sent from host A to host B, host A to host C, and host C to host B could all use different ports in the channel.

Related Topics

Configuring EtherChannel Load-Balancing (CLI), on page 157
EtherChannel Configuration Guidelines, on page 149
Layer 2 EtherChannel Configuration Guidelines, on page 150
Default EtherChannel Configuration, on page 148
Layer 3 EtherChannel Configuration Guidelines, on page 151

IP Address Forwarding

With source-IP address-based forwarding, packets are distributed across the ports in the EtherChannel based on the source-IP address of the incoming packet. To provide load balancing, packets from different IP addresses use different ports in the channel, and packets from the same IP address use the same port in the channel.

With destination-IP address-based forwarding, packets are distributed across the ports in the EtherChannel based on the destination-IP address of the incoming packet. To provide load balancing, packets from the same IP source address sent to different IP destination addresses could be sent on different ports in the channel.

Packets sent from different source IP addresses to the same destination IP address are always sent on the same port in the channel.

With source-and-destination IP address-based forwarding, packets are distributed across the ports in the EtherChannel based on both the source and destination IP addresses of the incoming packet. This forwarding method, a combination of source-IP and destination-IP address-based forwarding, can be used if it is not clear whether source-IP or destination-IP address-based forwarding is better suited on a particular switch. In this method, packets sent from the IP address A to IP address B, from IP address A to IP address C, and from IP address C to IP address B could all use different ports in the channel.

Related Topics

Configuring EtherChannel Load-Balancing (CLI), on page 157
EtherChannel Configuration Guidelines, on page 149
Layer 2 EtherChannel Configuration Guidelines, on page 150
Default EtherChannel Configuration, on page 148
Layer 3 EtherChannel Configuration Guidelines, on page 151

Load-Balancing Advantages

Different load-balancing methods have different advantages, and the choice of a particular load-balancing method should be based on the position of the switch in the network and the kind of traffic that needs to be load-distributed.

Figure 13: Load Distribution and Forwarding Methods

In the following figure, an EtherChannel of four workstations communicates with a router. Because the router is a single MAC-address device, source-based forwarding on the switch EtherChannel ensures that the switch uses all available bandwidth to the router. The router is configured for destination-based forwarding because the large number of workstations ensures that the traffic is evenly distributed from the router EtherChannel.

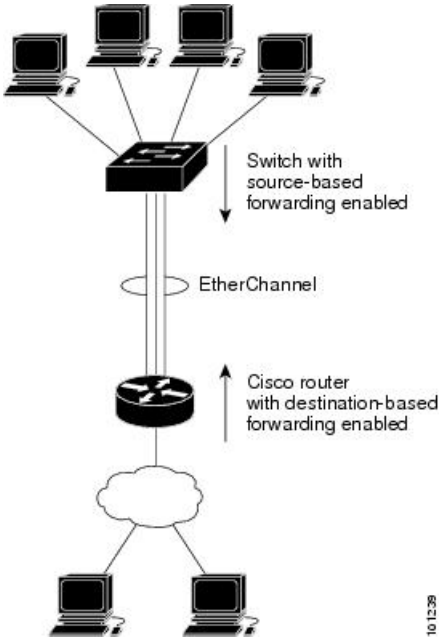
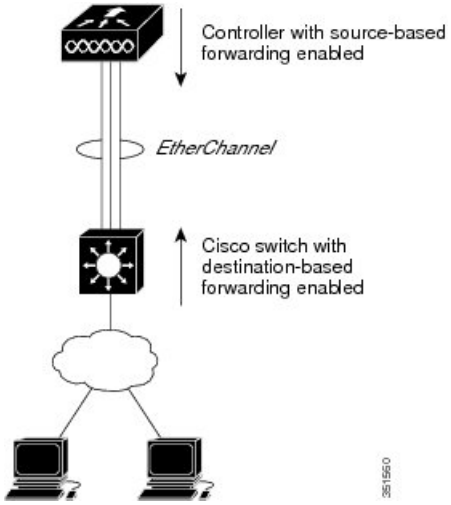


Figure 14: Load Distribution and Forwarding

In the figure below the controller does source MAC-based forwarding over the EtherChannel links and evenly distributes the traffic over multiple links of the EtherChannel.



Use the option that provides the greatest variety in your configuration. For example, if the traffic on a channel is going only to a single MAC address, using the destination-MAC address always chooses the same link in the channel. Using source addresses or IP addresses might result in better load-balancing.

Related Topics

Configuring EtherChannel Load-Balancing (CLI), on page 157
EtherChannel Configuration Guidelines, on page 149
Layer 2 EtherChannel Configuration Guidelines, on page 150
Default EtherChannel Configuration, on page 148
Layer 3 EtherChannel Configuration Guidelines, on page 151

EtherChannel and Switch Stacks

If a stack member that has ports participating in an EtherChannel fails or leaves the stack, the active switch removes the failed stack member switch ports from the EtherChannel. The remaining ports of the EtherChannel, if any, continue to provide connectivity.

When a switch is added to an existing stack, the new switch receives the running configuration from the active switch and updates itself with the EtherChannel-related stack configuration. The stack member also receives the operational information (the list of ports that are up and are members of a channel).

When two stacks merge that have EtherChannels configured between them, self-looped ports result. Spanning tree detects this condition and acts accordingly. Any PAgP or LACP configuration on a winning switch stack is not affected, but the PAgP or LACP configuration on the losing switch stack is lost after the stack reboots.

Switch Stack and PAgP

With PAgP, if the active switch fails or leaves the stack, the standby switch becomes the new active switch. A spanning-tree reconvergence is not triggered unless there is a change in the EtherChannel bandwidth. The new active switch synchronizes the configuration of the stack members to that of the active switch. The PAgP

configuration is not affected after an active switch change unless the EtherChannel has ports residing on the old active switch.

Switch Stacks and LACP

With LACP, the system ID uses the stack MAC address from the active switch. When an active switch fails or leaves the stack and the standby switch becomes the new active switch change, the LACP system ID is unchanged. By default, the LACP configuration is not affected after the active switch changes.

Default EtherChannel Configuration

The default EtherChannel configuration is described in this table.

Table 8: Default EtherChannel Configuration

Feature	Default Setting
Channel groups	None assigned.
Port-channel logical interface	None defined.
PAgP mode	No default.
PAgP learn method	Aggregate-port learning on all ports.
PAgP priority	128 on all ports.
LACP mode	No default.
LACP learn method	Aggregate-port learning on all ports.
LACP port priority	32768 on all ports.
LACP system priority	32768.
LACP system ID	LACP system priority and the switch or stack MAC address.
Load-balancing	Load distribution on the switch is based on the source-MAC address of the incoming packet.

Related Topics

Configuring Layer 2 EtherChannels (CLI), on page 153
EtherChannel Overview, on page 136
EtherChannel Modes, on page 136
EtherChannel on Switches, on page 137
EtherChannel Link Failover, on page 139
LACP Modes, on page 143
PAgP Modes , on page 140
Silent Mode, on page 141
Creating Port-Channel Logical Interfaces (CLI)
Channel Groups and Port-Channel Interfaces, on page 139

Configuring the Physical Interfaces (CLI)
Configuring EtherChannel Load-Balancing (CLI), on page 157
Load-Balancing and Forwarding Methods, on page 144
MAC Address Forwarding, on page 145
IP Address Forwarding, on page 145
Load-Balancing Advantages, on page 146
Configuring the PAgP Learn Method and Priority (CLI), on page 160
PAgP Learn Method and Priority, on page 141
Configuring the LACP System Priority (CLI), on page 164
Configuring the LACP Port Priority (CLI), on page 165

EtherChannel Configuration Guidelines

If improperly configured, some EtherChannel ports are automatically disabled to avoid network loops and other problems. Follow these guidelines to avoid configuration problems:

- Configure a PAgP EtherChannel with up to eight Ethernet ports of the same type.
- Configure a LACP EtherChannel with up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.
- Configure all ports in an EtherChannel to operate at the same speeds and duplex modes.
- Enable all ports in an EtherChannel. A port in an EtherChannel that is disabled by using the **shutdown** interface configuration command is treated as a link failure, and its traffic is transferred to one of the remaining ports in the EtherChannel.
- When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, you must also make the changes to all ports in the group:
  - Allowed-VLAN list
  - Spanning-tree path cost for each VLAN
  - Spanning-tree port priority for each VLAN
  - Spanning-tree Port Fast setting
- Do not configure a port to be a member of more than one EtherChannel group.
- Do not configure an EtherChannel in both the PAgP and LACP modes. EtherChannel groups running PAgP and LACP can coexist on the same switch or on different switches in the stack. Individual EtherChannel groups can run either PAgP or LACP, but they cannot interoperate.
- Do not configure a secure port as part of an EtherChannel or the reverse.
- Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an IEEE 802.1x port. If you try to enable IEEE 802.1x on an EtherChannel port, an error message appears, and IEEE 802.1x is not enabled.
- If EtherChannels are configured on switch interfaces, remove the EtherChannel configuration from the interfaces before globally enabling IEEE 802.1x on a switch by using the **dot1x system-auth-control** global configuration command.

- If cross-stack EtherChannel is configured and the switch stack partitions, loops and forwarding issues can occur.

Related Topics

Configuring Layer 2 EtherChannels (CLI), on page 153
EtherChannel Overview, on page 136
EtherChannel Modes, on page 136
EtherChannel on Switches, on page 137
EtherChannel Link Failover, on page 139
LACP Modes, on page 143
PAgP Modes , on page 140
Silent Mode, on page 141
Creating Port-Channel Logical Interfaces (CLI)
Channel Groups and Port-Channel Interfaces, on page 139
Configuring the Physical Interfaces (CLI)
Configuring EtherChannel Load-Balancing (CLI), on page 157
Load-Balancing and Forwarding Methods, on page 144
MAC Address Forwarding, on page 145
IP Address Forwarding, on page 145
Load-Balancing Advantages, on page 146
Configuring the PAgP Learn Method and Priority (CLI), on page 160
PAgP Learn Method and Priority, on page 141
Configuring the LACP System Priority (CLI), on page 164
Configuring the LACP Port Priority (CLI), on page 165

Layer 2 EtherChannel Configuration Guidelines

When configuring Layer 2 EtherChannels, follow these guidelines:

- Assign all ports in the EtherChannel to the same VLAN, or configure them as trunks. Ports with different native VLANs cannot form an EtherChannel.
- An EtherChannel supports the same allowed range of VLANs on all the ports in a trunking Layer 2 EtherChannel. If the allowed range of VLANs is not the same, the ports do not form an EtherChannel even when PAgP is set to the **auto** or **desirable** mode.
- Ports with different spanning-tree path costs can form an EtherChannel if they are otherwise compatibly configured. Setting different spanning-tree path costs does not, by itself, make ports incompatible for the formation of an EtherChannel.

Related Topics

Configuring Layer 2 EtherChannels (CLI), on page 153
EtherChannel Overview, on page 136
EtherChannel Modes, on page 136
EtherChannel on Switches, on page 137
EtherChannel Link Failover, on page 139
LACP Modes, on page 143
PAgP Modes , on page 140

Silent Mode, on page 141
Creating Port-Channel Logical Interfaces (CLI)
Channel Groups and Port-Channel Interfaces, on page 139
Configuring the Physical Interfaces (CLI)
Configuring EtherChannel Load-Balancing (CLI), on page 157
Load-Balancing and Forwarding Methods, on page 144
MAC Address Forwarding, on page 145
IP Address Forwarding, on page 145
Load-Balancing Advantages, on page 146
Configuring the PAgP Learn Method and Priority (CLI), on page 160
PAgP Learn Method and Priority, on page 141
Configuring the LACP System Priority (CLI), on page 164
Configuring the LACP Port Priority (CLI), on page 165

Layer 3 EtherChannel Configuration Guidelines

- For Layer 3 EtherChannels, assign the Layer 3 address to the port-channel logical interface, not to the physical ports in the channel.

Related Topics

Configuring EtherChannel Load-Balancing (CLI), on page 157
Load-Balancing and Forwarding Methods, on page 144
MAC Address Forwarding, on page 145
IP Address Forwarding, on page 145
Load-Balancing Advantages, on page 146

Auto-LAG

The auto-LAG feature provides the ability to auto create EtherChannels on ports connected to a switch. By default, auto-LAG is disabled globally and is enabled on all port interfaces. The auto-LAG applies to a switch only when it is enabled globally.

On enabling auto-LAG globally, the following scenarios are possible:

- All port interfaces participate in creation of auto EtherChannels provided the partner port interfaces have EtherChannel configured on them. For more information, see the *"The supported auto-LAG configurations between the actor and partner devices"* table below.
- Ports that are already part of manual EtherChannels cannot participate in creation of auto EtherChannels.
- When auto-LAG is disabled on a port interface that is already a part of an auto created EtherChannel, the port interface will unbundle from the auto EtherChannel.

The following table shows the supported auto-LAG configurations between the actor and partner devices:

Table 9: The supported auto-LAG configurations between the actor and partner devices

Actor/Partner	Active	Passive	Auto
Active	Yes	Yes	Yes

Passive	Yes	No	Yes
Auto	Yes	Yes	Yes

On disabling auto-LAG globally, all auto created Etherchannels become manual EtherChannels.

You cannot add any configurations in an existing auto created EtherChannel. To add, you should first convert it into a manual EtherChannel by executing the **port-channel**<*channel-number*>**persistent**.

Note Auto-LAG uses the LACP protocol to create auto EtherChannel. Only one EtherChannel can be automatically created with the unique partner devices.

Related Topics

Configuring Auto-LAG Globally, on page 166
Configuring Auto LAG: Examples, on page 172
Configuring Auto-LAG on a Port Interface, on page 167
Configuring Persistence with Auto-LAG, on page 168
Auto-LAG Configuration Guidelines, on page 152

Auto-LAG Configuration Guidelines

Follow these guidelines when configuring the auto-LAG feature.

- When auto-LAG is enabled globally and on the port interface , and if you do not want the port interface to become a member of the auto EtherChannel, disable the auto-LAG on the port interface.
- A port interface will not bundle to an auto EtherChannel when it is already a member of a manual EtherChannel. To allow it to bundle with the auto EtherChannel, first unbundle the manual EtherChannel on the port interface.
- When auto-LAG is enabled and auto EtherChannel is created, you can create multiple EtherChannels manually with the same partner device. But by default, the port tries to create auto EtherChannel with the partner device.
- The auto-LAG is supported only on Layer 2 EtherChannel. It is not supported on Layer 3 interface and Layer 3 EtherChannel.
- The auto-LAG is supported on cross-stack EtherChannel.

Related Topics

Configuring Auto-LAG Globally, on page 166
Configuring Auto LAG: Examples, on page 172
Configuring Auto-LAG on a Port Interface, on page 167
Configuring Persistence with Auto-LAG, on page 168
Auto-LAG, on page 151

How to Configure EtherChannels

After you configure an EtherChannel, configuration changes applied to the port-channel interface apply to all the physical ports assigned to the port-channel interface, and configuration changes applied to the physical port affect only the port where you apply the configuration.

Configuring Layer 2 EtherChannels (CLI)

You configure Layer 2 EtherChannels by assigning ports to a channel group with the **channel-group** interface configuration command. This command automatically creates the port-channel logical interface.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet2/0/1`	Specifies a physical port, and enters interface configuration mode. Valid interfaces are physical ports. For a PAgP EtherChannel, you can configure up to eight ports of the same type and speed for the same group. For a LACP EtherChannel, you can configure up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.
Step 3	**switchport mode** {**access** | **trunk**} **Example:** `Switch(config-if)# switchport mode access`	Assigns all ports as static-access ports in the same VLAN, or configure them as trunks. If you configure the port as a static-access port, assign it to only one VLAN. The range is 1 to 4094.
Step 4	**switchport access vlan** *vlan-id* **Example:** `Switch(config-if)# switchport access vlan 22`	(Optional) If you configure the port as a static-access port, assign it to only one VLAN. The range is 1 to 4094.

	Command or Action	Purpose
Step 5	**channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on** } | { **active** | **passive**} **Example:** `Switch(config-if)# channel-group 5 mode auto`	Assigns the port to a channel group, and specifies the PAgP or the LACP mode. For *channel-group-number*, the range is 1 to 128. For **mode**, select one of these keywords: • **auto** –Enables PAgP only if a PAgP device is detected. It places the port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation.This keyword is not supported when EtherChannel members are from different switches in the switch stack. • **desirable** –Unconditionally enables PAgP. It places the port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets. This keyword is not supported when EtherChannel members are from different switches in the switch stack. • **on** –Forces the port to channel without PAgP or LACP. In the **on** mode, an EtherChannel exists only when a port group in the **on** mode is connected to another port group in the **on** mode. • **non-silent** –(Optional) If your switch is connected to a partner that is PAgP-capable, configures the switch port for nonsilent operation when the port is in the **auto** or **desirable** mode. If you do not specify **non-silent**, silent is assumed. The silent setting is for connections to file servers or packet analyzers. This setting allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission. • **active**—Enables LACP only if a LACP device is detected. It places the port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets. • **passive** –Enables LACP on the port and places it into a passive negotiating state in which the port responds to LACP packets

	Command or Action	Purpose
		that it receives, but does not start LACP packet negotiation.
Step 6	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Related Topics

EtherChannel Overview, on page 136
EtherChannel Modes, on page 136
EtherChannel on Switches, on page 137
EtherChannel Link Failover, on page 139
LACP Modes, on page 143
PAgP Modes , on page 140
Silent Mode, on page 141
EtherChannel Configuration Guidelines, on page 149
Default EtherChannel Configuration, on page 148
Layer 2 EtherChannel Configuration Guidelines, on page 150

Configuring Layer 3 EtherChannels (CLI)

Follow these steps to assign an Ethernet port to a Layer 3 EtherChannel. This procedure is required.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet`	Specifies a physical port, and enters interface configuration mode. Valid interfaces include physical ports.

	Command or Action	Purpose
	`1/0/2`	For a PAgP EtherChannel, you can configure up to eight ports of the same type and speed for the same group. For a LACP EtherChannel, you can configure up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.
Step 4	**no ip address** **Example:** `Switch(config-if)# no ip address`	Ensures that there is no IP address assigned to the physical port.
Step 5	**no switchport** **Example:** `Switch(config-if)# no switchport`	Puts the port into Layer 3 mode.
Step 6	**channel-group** *channel-group-number* **mode** { **auto** [**non-silent**] | **desirable** [**non-silent**] | **on** } | { **active** | **passive** } **Example:** `Switch(config-if)# channel-group 5 mode auto`	Assigns the port to a channel group, and specifies the PAgP or the LACP mode. For **mode**, select one of these keywords: • **auto**—Enables PAgP only if a PAgP device is detected. It places the port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. This keyword is not supported when EtherChannel members are from different switches in the switch stack. • **desirable**—Unconditionally enables PAgP. It places the port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets. This keyword is not supported when EtherChannel members are from different switches in the switch stack. • **on**—Forces the port to channel without PAgP or LACP. In the **on** mode, an EtherChannel exists only when a port group in the **on** mode is connected to another port group in the **on** mode. • **non-silent**—(Optional) If your switch is connected to a partner that is PAgP

	Command or Action	Purpose
		capable, configures the switch port for nonsilent operation when the port is in the **auto** or **desirable** mode. If you do not specify **non-silent**, silent is assumed. The silent setting is for connections to file servers or packet analyzers. This setting allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission. • **active**—Enables LACP only if a LACP device is detected. It places the port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets. • **passive** –Enables LACP on the port and places it into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation.
Step 7	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Configuring EtherChannel Load-Balancing (CLI)

You can configure EtherChannel load-balancing to use one of several different forwarding methods.

This task is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**port-channel load-balance** { **dst-ip** | **dst-mac** | **dst-mixed-ip-port** | **dst-port** | **extended** [**dst-ip** | **dst-mac** | **dst-port** | **ipv6-label** | **l3-proto** | **src-ip** | **src-mac** | **src-port**] |	Configures an EtherChannel load-balancing method. The default is **src-mac**. Select one of these load-distribution methods:

	Command or Action	Purpose
	src-dst-ip | **src-dst-mac** **src-dst-mixed-ip-port src-dst-portsrc-ip** | **src-mac** | **src-mixed-ip-port** | **src-port**} **Example:** `Switch(config)# port-channel load-balance src-mac`	• **dst-ip**—Specifies destination-host IP address. • **dst-mac**—Specifies the destination-host MAC address of the incoming packet. • **dst-mixed-ip-port**—Specifies the host IP address and TCP/UDP port. • **dst-port**—Specifies the destination TCP/UDP port. • **extended**—Specifies extended load balance methods--combinations of source and destination methods beyond those available with the standard command. • **ipv6-label**—Specifies the IPv6 flow label. • **l3-proto**—Specifies the Layer 3 protocol. • **src-dst-ip**—Specifies the source and destination host IP address. • **src-dst-mac**—Specifies the source and destination host MAC address. • **src-dst-mixed-ip-port**—Specifies the source and destination host IP address and TCP/UDP port. • **src-dst-port**—Specifies the source and destination TCP/UDP port. • **src-ip**—Specifies the source host IP address. • **src-mac**—Specifies the source MAC address of the incoming packet. • **src-mixed-ip-port**—Specifies the source host IP address and TCP/UDP port. • **src-port**—Specifies the source TCP/UDP port.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Related Topics

Load-Balancing and Forwarding Methods, on page 144

MAC Address Forwarding, on page 145
IP Address Forwarding, on page 145
Load-Balancing Advantages, on page 146
EtherChannel Configuration Guidelines, on page 149
Layer 2 EtherChannel Configuration Guidelines, on page 150
Default EtherChannel Configuration, on page 148
Layer 3 EtherChannel Configuration Guidelines, on page 151

Configuring EtherChannel Extended Load-Balancing (CLI)

Configure EtherChannel extended load-balancing when you want to use a combination of load-balancing methods.

This task is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**port-channel load-balance extended** [**dst-ip** | **dst-mac dst-port** | **ipv6-label** | **l3-proto** | **src-ip** | **src-mac** | **src-port**] **Example:** `Switch(config)# port-channel load-balance extended dst-ip dst-mac src-ip`	Configures an EtherChannel extended load-balancing method. The default is **src-mac**. Select one of these load-distribution methods: • **dst-ip**—Specifies destination-host IP address. • **dst-mac**—Specifies the destination-host MAC address of the incoming packet. • **dst-port**—Specifies the destination TCP/UDP port. • **ipv6-label**—Specifies the IPv6 flow label. • **l3-proto**—Specifies the Layer 3 protocol. • **src-ip**—Specifies the source host IP address. • **src-mac**—Specifies the source MAC address of the incoming packet. • **src-port**—Specifies the source TCP/UDP port.

	Command or Action	Purpose
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Configuring the PAgP Learn Method and Priority (CLI)

This task is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/2`	Specifies the port for transmission, and enters interface configuration mode.
Step 3	**pagp learn-method physical-port** **Example:** `Switch(config-if)# pagp learn-method physical port`	Selects the PAgP learning method. By default, **aggregation-port learning** is selected, which means the switch sends packets to the source by using any of the ports in the EtherChannel. With aggregate-port learning, it is not important on which physical port the packet arrives. Selects **physical-port** to connect with another switch that `is` a physical learner. Make sure to configure the **port-channel load-balance** global configuration command to **src-mac**. The learning method must be configured the same at both ends of the link.
Step 4	**pagp port-priority** *priority* **Example:**	Assigns a priority so that the selected port is chosen for packet transmission.

	Command or Action	Purpose
	`Switch(config-if)# pagp port-priority 200`	For *priority*, the range is 0 to 255. The default is 128. The higher the priority, the more likely that the port will be used for PAgP transmission.
Step 5	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Related Topics

PAgP Learn Method and Priority, on page 141
EtherChannel Configuration Guidelines, on page 149
Default EtherChannel Configuration, on page 148
Monitoring EtherChannel, PAgP, and LACP Status, on page 169
Layer 2 EtherChannel Configuration Guidelines, on page 150

Configuring LACP Hot-Standby Ports

When LACP is enabled, the software, by default, tries to configure the maximum number of LACP-compatible ports in a channel, up to a maximum of 16 ports. Only eight LACP links can be active at one time; the remaining eight links are placed in hot-standby mode. If one of the active links becomes inactive, a link that is in the hot-standby mode becomes active in its place.

You can override the default behavior by specifying the maximum number of active ports in a channel, in which case, the remaining ports become hot-standby ports. For example, if you specify a maximum of five ports in a channel, up to 11 ports become hot-standby ports.

If you configure more than eight links for an EtherChannel group, the software automatically decides which of the hot-standby ports to make active based on the LACP priority. To every link between systems that operate LACP, the software assigns a unique priority made up of these elements (in priority order):

- LACP system priority
- System ID (the switch MAC address)
- LACP port priority
- Port number

In priority comparisons, numerically lower values have higher priority. The priority decides which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

Determining which ports are active and which are hot standby is a two-step procedure. First the system with a numerically lower system priority and system ID is placed in charge of the decision. Next, that system decides which ports are active and which are hot standby, based on its values for port priority and port number. The port priority and port number values for the other system are not used.

You can change the default values of the LACP system priority and the LACP port priority to affect how the software selects active and standby links.

Configuring the LACP Max Bundle Feature (CLI)

When you specify the maximum number of bundled LACP ports allowed in a port channel, the remaining ports in the port channel are designated as hot-standby ports.

Beginning in privileged EXEC mode, follow these steps to configure the maximum number of LACP ports in a port channel. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**interface port-channel** *channel-number* **Example:** `Switch(config)# interface port-channel 2`	Enters interface configuration mode for a port channel. The range is 1 to 128.
Step 3	**lacp max-bundle** *max-bundle-number* **Example:** `Switch(config-if)# lacp max-bundle 3`	Specifies the maximum number of LACP ports in the port-channel bundle. The range is 1 to 8.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Related Topics

LACP and Link Redundancy , on page 143
Configuring LACP Hot-Standby Ports: Example, on page 172

Configuring LACP Port-Channel Standalone Disable

To disable the standalone EtherChannel member port state on a port channel, perform this task on the port channel interface:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface port-channel** *channel-group* **Example:** `Switch(config)# interface port-channel channel-group`	Selects a port channel interface to configure.
Step 3	**port-channel standalone-disable** **Example:** `Switch(config-if)# port-channel standalone-disable`	Disables the standalone mode on the port-channel interface.
Step 4	**end** **Example:** `Switch(config-if)# end`	Exits configuration mode.

Step 5	**show etherchannel**
	Example:
	`Switch# show etherchannel channel-group port-channel`
	`Switch# show etherchannel channel-group detail`
		Verifies the configuration.

Related Topics

Configuring LACP Hot-Standby Ports: Example, on page 172

Configuring the LACP Port Channel Min-Links Feature (CLI)

You can specify the minimum number of active ports that must be in the link-up state and bundled in an EtherChannel for the port channel interface to transition to the link-up state. Using EtherChannel min-links, you can prevent low-bandwidth LACP EtherChannels from becoming active. Port channel min-links also cause LACP EtherChannels to become inactive if they have too few active member ports to supply the requiredminimum bandwidth.

To configure the minimum number of links that are required for a port channel. Perform the following tasks.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Switch> enable`	
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**interface port-channel** *channel-number* **Example:** `Switch(config)# interface port-channel 2`	Enters interface configuration mode for a port-channel. For *channel-number*, the range is 1 to 63.
Step 4	**port-channel min-links** *min-links-number* **Example:** `Switch(config-if)# port-channel min-links 3`	Specifies the minimum number of member ports that must be in the link-up state and bundled in the EtherChannel for the port channel interface to transition to the link-up state. For *min-links-number* , the range is 2 to 8.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Related Topics

LACP and Link Redundancy , on page 143
Configuring LACP Hot-Standby Ports: Example, on page 172

Configuring the LACP System Priority (CLI)

You can configure the system priority for all the EtherChannels that are enabled for LACP by using the **lacp system-priority** global configuration command. You cannot configure a system priority for each LACP-configured channel. By changing this value from the default, you can affect how the software selects active and standby links.

You can use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag).

Follow these steps to configure the LACP system priority. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Switch> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**lacp system-priority** *priority* **Example:** `Switch(config)# lacp system-priority 32000`	Configures the LACP system priority. The range is 1 to 65535. The default is 32768. The lower the value, the higher the system priority.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Related Topics

EtherChannel Configuration Guidelines, on page 149
Default EtherChannel Configuration, on page 148
Layer 2 EtherChannel Configuration Guidelines, on page 150
Monitoring EtherChannel, PAgP, and LACP Status, on page 169

Configuring the LACP Port Priority (CLI)

By default, all ports use the same port priority. If the local system has a lower value for the system priority and the system ID than the remote system, you can affect which of the hot-standby links become active first by changing the port priority of LACP EtherChannel ports to a lower value than the default. The hot-standby ports that have lower port numbers become active in the channel first. You can use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag).

Note If LACP is not able to aggregate all the ports that are compatible (for example, the remote system might have more restrictive hardware limitations), all the ports that cannot be actively included in the EtherChannel are put in the hot-standby state and are used only if one of the channeled ports fails.

Follow these steps to configure the LACP port priority. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/2`	Specifies the port to be configured, and enters interface configuration mode.
Step 4	**lacp port-priority** *priority* **Example:** `Switch(config-if)# lacp port-priority 32000`	Configures the LACP port priority. The range is 1 to 65535. The default is 32768. The lower the value, the more likely that the port will be used for LACP transmission.
Step 5	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Related Topics

EtherChannel Configuration Guidelines, on page 149
Default EtherChannel Configuration, on page 148
Layer 2 EtherChannel Configuration Guidelines, on page 150
Monitoring EtherChannel, PAgP, and LACP Status, on page 169

Configuring Auto-LAG Globally

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Switch> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**[no] port-channel auto** **Example:** `Switch(config)# port-channel auto`	Enables the auto-LAG feature on a switch globally. Use the no form of this command to disable the auto-LAG feature on the switch globally. **Note** By default, the auto-LAG feature is enabled on the port.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show etherchannel auto** **Example:** `Switch# show etherchannel auto`	Displays that EtherChannel is created automatically.

Related Topics

Auto-LAG, on page 151
Auto-LAG Configuration Guidelines, on page 152
Configuring Auto LAG: Examples, on page 172
Configuring Auto-LAG on a Port Interface, on page 167
Configuring Persistence with Auto-LAG, on page 168

Configuring Auto-LAG on a Port Interface

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Specifies the port interface to be enabled for auto-LAG, and enters interface configuration mode.
Step 4	[**no**] **channel-group auto** **Example:** `Switch(config-if)# channel-group auto`	(Optional) Enables auto-LAG feature on individual port interface. Use the no form of this command to disable the auto-LAG feature on individual port interface. **Note** By default, the auto-LAG feature is enabled on the port.
Step 5	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show etherchannel auto** **Example:** `Switch# show etherchannel auto`	Displays that EtherChannel is created automatically.

What to do next

Related Topics

Configuring Auto-LAG Globally, on page 166
Auto-LAG, on page 151
Auto-LAG Configuration Guidelines, on page 152
Configuring Persistence with Auto-LAG, on page 168
Configuring Auto LAG: Examples, on page 172

Configuring Persistence with Auto-LAG

You use the persistence command to convert the auto created EtherChannel into a manual one and allow you to add configuration on the existing EtherChannel.

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Switch> enable`	• Enter your password if prompted.
Step 2	**port-channel** *channel-number* **persistent** **Example:** `Switch# port-channel 1 persistent`	Converts the auto created EtherChannel into a manual one and allows you to add configuration on the EtherChannel.
Step 3	**show etherchannel summary** **Example:** `Switch# show etherchannel summary`	Displays the EtherChannel information.

Related Topics

Configuring Auto-LAG Globally, on page 166
Auto-LAG, on page 151
Auto-LAG Configuration Guidelines, on page 152
Configuring Auto-LAG on a Port Interface, on page 167
Configuring Auto LAG: Examples, on page 172

Monitoring EtherChannel, PAgP, and LACP Status

You can display EtherChannel, PAgP, and LACP status using the commands listed in this table.

Table 10: Commands for Monitoring EtherChannel, PAgP, and LACP Status

Command	Description
clear lacp { *channel-group-number* **counters** | **counters** }	Clears LACP channel-group information and traffic counters.
clear pagp { *channel-group-number* **counters** | **counters** }	Clears PAgP channel-group information and traffic counters.
show etherchannel [*channel-group-number* { **detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary** }] [**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **auto** | **summary**]	Displays EtherChannel information in a brief, detailed, and one-line summary form. Also displays the load-balance or frame-distribution scheme, port, port-channel, protocol, and Auto-LAG information.
show pagp [*channel-group-number*] { **counters** | **internal** | **neighbor** }	Displays PAgP information such as traffic information, the internal PAgP configuration, and neighbor information.
show pagp [*channel-group-number*] **dual-active**	Displays the dual-active detection status.

Command	Description
show lacp [*channel-group-number*] { **counters** | **internal** | **neighbor** | **sys-id**}	Displays LACP information such as traffic information, the internal LACP configuration, and neighbor information.
show running-config	Verifies your configuration entries.
show etherchannel load-balance	Displays the load balance or frame distribution scheme among ports in the port channel.

Related Topics

Configuring the PAgP Learn Method and Priority (CLI), on page 160
PAgP Learn Method and Priority, on page 141
Configuring the LACP System Priority (CLI), on page 164
Configuring the LACP Port Priority (CLI), on page 165

Configuration Examples for Configuring EtherChannels

Configuring Layer 2 EtherChannels: Examples

This example shows how to configure an EtherChannel on a single switch in the stack. It assigns two ports as static-access ports in VLAN 10 to channel 5 with the PAgP mode **desirable**:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable non-silent
Switch(config-if-range)# end
```

This example shows how to configure an EtherChannel on a single switch in the stack. It assigns two ports as static-access ports in VLAN 10 to channel 5 with the LACP mode **active**:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

This example shows how to configure a cross-stack EtherChannel. It uses LACP passive mode and assigns two ports on stack member 1 and one port on stack member 2 as static-access ports in VLAN 10 to channel 5:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/4 -5
Switch(config-if-range)# switchport mode access
```

```
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode passive
Switch(config-if-range)# exit
Switch(config)# interface gigabitethernet3/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# channel-group 5 mode passive
Switch(config-if)# exit
```

PoE or LACP negotiation errors may occur if you configure two ports from switch to the access point (AP). This scenario can be avoided if the port channel configuration is on the switch side. For more details, see the following example:

```
interface Port-channel1
  switchport access vlan 20
 switchport mode access
  switchport nonegotiate
  no port-channel standalone-disable   <--this one
  spanning-tree portfast
```

Note If the port reports LACP errors on port flap, you should include the following command as well: **no errdisable detect cause pagp-flap**

Configuring Layer 3 EtherChannels: Examples

This example shows how to configure a Layer 3 EtherChannel. It assigns two ports to channel 5 with the LACP mode **active**:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# no ip address
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

This example shows how to configure a cross-stack Layer 3 EtherChannel. It assigns two ports on stack member 2 and one port on stack member 3 to channel 7 using LACP active mode:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/4 -5
Switch(config-if-range)# no ip address
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 7 mode active
Switch(config-if-range)# exit
Switch(config)# interface gigabitethernet3/0/3
Switch(config-if)# no ip address
Switch(config-if)# no switchport
Switch(config-if)# channel-group 7 mode active
Switch(config-if)# exit
```

Configuring LACP Hot-Standby Ports: Example

This example shows how to configure an Etherchannel (port channel 2) that will be active when there are at least three active ports, will comprise up to seven active ports and the remaining ports (up to nine) as hot-standby ports :

```
Switch# configure terminal
Switch(config)# interface port-channel 2
Switch(config-if)# port-channel min-links 3
Switch(config-if)# lacp max-bundle 7
```

This example shows how to disable the standalone EtherChannel member port state on port channel 42:

```
Switch(config)# interface port-channel channel-group
Switch(config-if)# port-channel standalone-disable
```

This example shows how to verify the configuration:

```
Switch# show etherchannel 42 port-channel | include Standalone
Standalone Disable  = enabled
Switch# show etherchannel 42 detail | include Standalone
Standalone Disable  = enabled
```

Related Topics

Configuring the LACP Max Bundle Feature (CLI), on page 162
LACP and Link Redundancy , on page 143
Configuring LACP Port-Channel Standalone Disable, on page 162
Configuring the LACP Port Channel Min-Links Feature (CLI), on page 163

Configuring Auto LAG: Examples

This example shows how to configure Auto-LAG on a switch

```
switch> enable
switch# configure terminal
switch (config)# port-channel auto
switch (config-if)# end
switch#  show etherchannel auto
```

The following example shows the summary of EtherChannel that was created automatically.

```
switch# show etherchannel auto
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
```

```
------+-------------+-----------+-----------------------------------------------
1      Po1(SUA)         LACP      Gi1/0/45(P) Gi2/0/21(P) Gi3/0/21(P)
```

The following example shows the summary of auto EtherChannel after executing the **port-channel** 1 **persistent** command.

```
switch# port-channel 1 persistent

switch# show etherchannel summary
Switch# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Gi1/0/45(P) Gi2/0/21(P) Gi3/0/21(P)
```

Related Topics

Configuring Auto-LAG Globally, on page 166
Auto-LAG, on page 151
Auto-LAG Configuration Guidelines, on page 152
Configuring Persistence with Auto-LAG, on page 168
Configuring Auto-LAG on a Port Interface, on page 167

Additional References for EtherChannels

Related Documents

Related Topic	Document Title
Layer 2 command reference	*Layer 2/3 Command Reference (Catalyst 3850 Switches)Layer 2 Command Reference (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

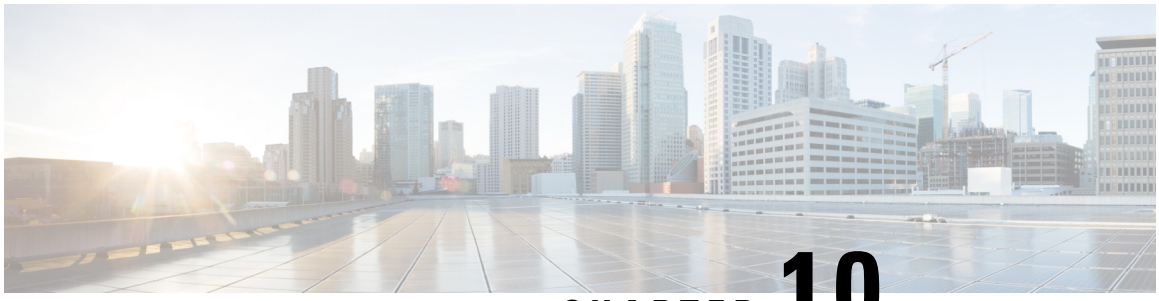
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for EtherChannels

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.
Cisco IOS XE 3.3SE	Support for the LACP max-bundle feature and the port channel min-links features was added.
Cisco IOS 15.2(3)E2, Cisco IOS XE 3.7.2E	Auto-LAG feature was introduced.



CHAPTER 10

Configuring Flex Links and the MAC Address-Table Move Update Feature

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring Flex Links and MAC Address-Table Move Update

- Flex Links are supported only on Layer 2 ports and port channels.
- You can configure up to 16 backup links.
- You can configure only one Flex Links backup link for any active link, and it must be a different interface from the active interface.

- An interface can belong to only one Flex Links pair. An interface can be a backup link for only one active link. An active link cannot belong to another Flex Links pair.
- Neither of the links can be a port that belongs to an EtherChannel. However, you can configure two port channels (EtherChannel logical interfaces) as Flex Links, and you can configure a port channel and a physical interface as Flex Links, with either the port channel or the physical interface as the active link.
- A backup link does not have to be the same type (Gigabit Ethernet or port channel) as the active link. However, you should configure both Flex Links with similar characteristics so that there are no loops or changes in behavior if the standby link begins to forward traffic.
- STP is disabled on Flex Links ports. A Flex Links port does not participate in STP, even if the VLANs present on the port are configured for STP. When STP is not enabled, be sure that there are no loops in the configured topology.
- You cannot have a switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches.

Related Topics

Configuring a Preemption Scheme for a Pair of Flex Links (CLI), on page 183
Configuring Flex Links (CLI), on page 182
Configuring Flex Links: Examples, on page 188
Configuring VLAN Load Balancing on Flex Links (CLI), on page 185
Configuring VLAN Load Balancing on Flex Links: Examples, on page 189
Configuring a Switch to Obtain and Process MAC Address-Table Move Update Messages (CLI), on page 187
Configuring MAC Address-Table Move Update (CLI), on page 186
Configuring the MAC Address-Table Move Update: Examples, on page 190

Information About Flex Links and MAC Address-Table Move Update

Flex Links

Flex Links are a pair of a Layer 2 interfaces (switch ports or port channels) where one interface is configured to act as a backup to the other. The feature provides an alternative solution to the Spanning Tree Protocol (STP). Users can disable STP and still retain basic link redundancy. Flex Links are typically configured in service provider or enterprise networks where customers do not want to run STP on the switch. If the switch is running STP, Flex Links are not necessary because STP already provides link-level redundancy or backup.

You configure Flex Links on one Layer 2 interface (the active link) by assigning another Layer 2 interface as the Flex Links or backup link. On switches, the Flex Links can be on the same switch or on another switch in the stack. When one of the links is up and forwarding traffic, the other link is in standby mode, ready to begin forwarding traffic if the other link shuts down. At any given time, only one of the interfaces is in the linkup state and forwarding traffic. If the primary link shuts down, the standby link starts forwarding traffic. When the active link comes back up, it goes into standby mode and does not forward traffic. STP is disabled on Flex Links interfaces.

Related Topics

Configuring a Preemption Scheme for a Pair of Flex Links (CLI), on page 183

Configuring Flex Links (CLI), on page 182
Configuring Flex Links: Examples, on page 188

Flex Links Configuration

In the following figure, ports 1 and 2 on switch A are connected to uplink switches B and C. Because they are configured as Flex Links, only one of the interfaces is forwarding traffic; the other is in standby mode. If port 1 is the active link, it begins forwarding traffic between port 1 and switch B; the link between port 2 (the backup link) and switch C is not forwarding traffic. If port 1 goes down, port 2 comes up and starts forwarding traffic to switch C. When port 1 comes back up, it goes into standby mode and does not forward traffic; port 2 continues forwarding traffic.

You can also configure a preemption function, specifying the preferred port for forwarding traffic. For example, you can configure the Flex Links pair with preemption mode. In the scenario shown, when port 1 comes back up and has more bandwidth than port 2, port 1 begins forwarding traffic after 60 seconds. Port 2 becomes the standby port. You do this by entering the **switchport backup interface preemption mode bandwidth** and **switchport backup interface preemption delay** interface configuration commands.

Figure 15: Flex Links Configuration Example

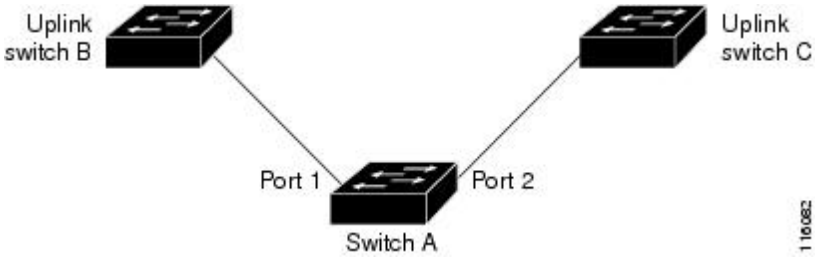
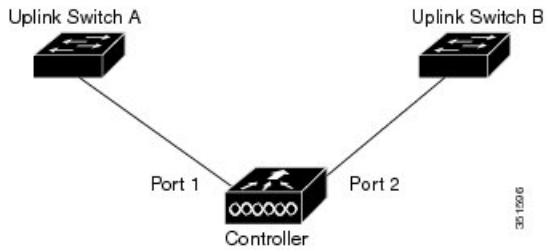


Figure 16: Flex Links Configuration Example



If a primary (forwarding) link goes down, a trap notifies the network management stations. If the standby link goes down, a trap notifies the users.

Flex Links are supported only on Layer 2 ports and port channels, not on VLANs or on Layer 3 ports.

Related Topics

Configuring a Preemption Scheme for a Pair of Flex Links (CLI), on page 183
Configuring Flex Links (CLI), on page 182

VLAN Flex Links Load Balancing and Support

VLAN Flex Links load balancing allows users to configure a Flex Links pair so that both ports simultaneously forward the traffic for some mutually exclusive VLANs. For example, if Flex Links ports are configured for 1 to 100 VLANs, the traffic of the first 50 VLANs can be forwarded on one port and the rest on the other

port. If one of the ports fail, the other active port forwards all the traffic. When the failed port comes back up, it resumes forwarding traffic in the preferred VLANs. In addition to providing the redundancy, this Flex Links pair can be used for load balancing. Flex Links VLAN load balancing does not impose any restrictions on uplink switches.

Figure 17: VLAN Flex Links Load-Balancing Configuration Example

The following figure displays a VLAN Flex Links load-balancing configuration.

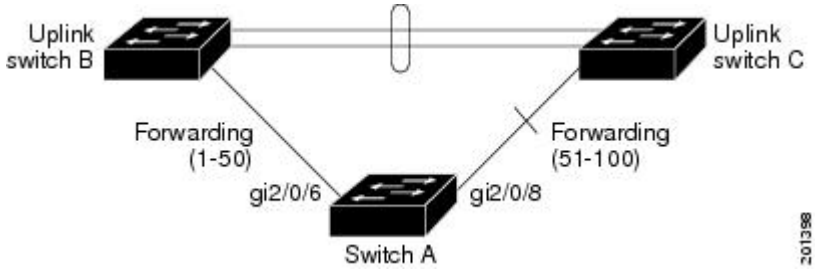
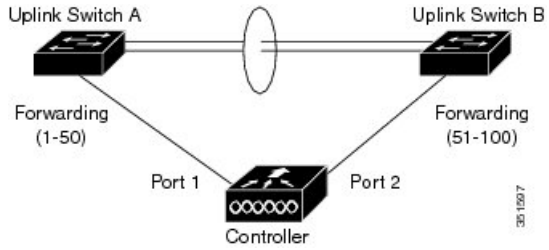


Figure 18: VLAN Flex Links Load-Balancing Configuration Example



Multicast Fast Convergence with Flex Links Failover

Multicast fast convergence reduces the multicast traffic convergence time after a Flex Links failure. Multicast fast convergence is implemented by a combination of learning the backup link as an mrouter port, generating IGMP reports, and leaking IGMP reports.

Related Topics

Configuring Multicast Fast Convergence with Flex Links Failover: Examples, on page 191

Learning the Other Flex Links Port as the mrouter Port

In a typical multicast network, there is a querier for each VLAN. A switch deployed at the edge of a network has one of its Flex Links ports receiving queries. Flex Links ports are also always forwarding at any given time.

A port that receives queries is added as an mrouter port on the switch. An mrouter port is part of all the multicast groups learned by the switch. After a changeover, queries are received by the other Flex Links port. The other Flex Links port is then learned as the mrouter port. After changeover, multicast traffic then flows through the other Flex Links port. To achieve faster convergence of traffic, both Flex Links ports are learned as mrouter ports whenever either Flex Links port is learned as the mrouter port. Both Flex Links ports are always part of multicast groups.

Although both Flex Links ports are part of the groups in normal operation mode, all traffic on the backup port is blocked. The normal multicast data flow is not affected by the addition of the backup port as an mrouter

port. When the changeover happens, the backup port is unblocked, allowing the traffic to flow. In this case, the upstream multicast data flows as soon as the backup port is unblocked.

Generating IGMP Reports

When the backup link comes up after the changeover, the upstream new distribution switch does not start forwarding multicast data, because the port on the upstream router, which is connected to the blocked Flex Links port, is not part of any multicast group. The reports for the multicast groups were not forwarded by the downstream switch because the backup link is blocked. The data does not flow on this port, until it learns the multicast groups, which occurs only after it receives reports.

The reports are sent by hosts when a general query is received, and a general query is sent within 60 seconds in normal scenarios. When the backup link starts forwarding, to achieve faster convergence of multicast data, the downstream switch immediately sends proxy reports for all the learned groups on this port without waiting for a general query.

Leaking IGMP Reports

To achieve multicast traffic convergence with minimal loss, a redundant data path must be set up before the Flex Links active link goes down. This can be achieved by leaking only IGMP report packets on the Flex Links backup link. These leaked IGMP report messages are processed by upstream distribution routers, so multicast data traffic gets forwarded to the backup interface. Because all incoming traffic on the backup interface is dropped at the ingress of the access switch, no duplicate multicast traffic is received by the host. When the Flex Links active link fails, the access switch starts accepting traffic from the backup link immediately. The only disadvantage of this scheme is that it consumes bandwidth on the link between the distribution switches and on the backup link between the distribution and access switches. This feature is disabled by default and can be configured by using the **switchport backup interface** *interface-id* **multicast fast-convergence** command.

When this feature has been enabled at changeover, the switch does not generate the proxy reports on the backup port, which became the forwarding port.

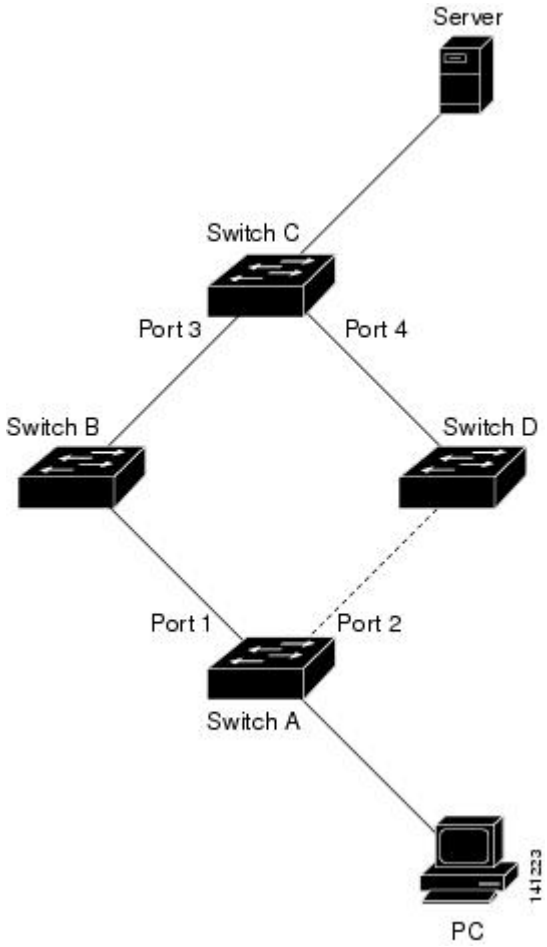
MAC Address-Table Move Update

The MAC address-table move update feature allows the switch to provide rapid bidirectional convergence when a primary (forwarding) link goes down and the standby link begins forwarding traffic.

Figure 19: MAC Address-Table Move Update Example

In the following figure, switch A is an access switch, and ports 1 and 2 on switch A are connected to uplink switches B and D through a Flex Links pair. Port 1 is forwarding traffic, and port 2 is in the backup state. Traffic from the PC to the server is forwarded from port 1 to port 3. The MAC address of the PC has been

learned on port 3 of switch C. Traffic from the server to the PC is forwarded from port 3 to port 1.



If the MAC address-table move update feature is not configured and port 1 goes down, port 2 starts forwarding traffic. However, for a short time, switch C keeps forwarding traffic from the server to the PC through port 3, and the PC does not get the traffic because port 1 is down. If switch C removes the MAC address of the PC on port 3 and relearns it on port 4, traffic can then be forwarded from the server to the PC through port 2.

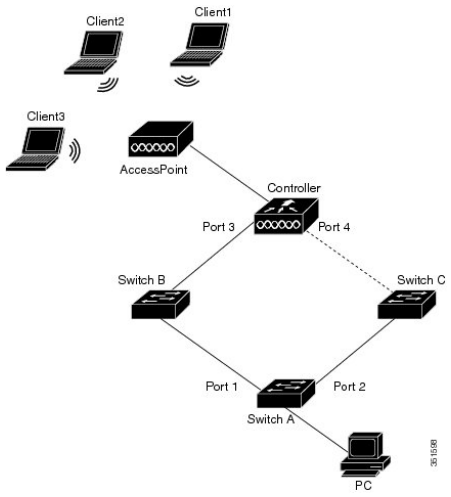
If the MAC address-table move update feature is configured and enabled on the switches, and port 1 goes down, port 2 starts forwarding traffic from the PC to the server. The switch sends a MAC address-table move update packet from port 2. Switch C gets this packet on port 4 and immediately learns the MAC address of the PC on port 4, which reduces the reconvergence time.

You can configure the access switch, switch A, to *send* MAC address-table move update messages. You can also configure the uplink switches B, C, and D to *get* and process the MAC address-table move update messages. When switch C gets a MAC address-table move update message from switch A, switch C learns the MAC address of the PC on port 4. Switch C updates the MAC address table, including the forwarding table entry for the PC.

Switch A does not need to wait for the MAC address-table update. The switch detects a failure on port 1 and immediately starts forwarding server traffic from port 2, the new forwarding port. This change occurs in less than 100 milliseconds (ms). The PC is directly connected to switch A, and the connection status does not change. Switch A does not need to update the PC entry in the MAC address table.

Figure 20: MAC Address-Table Move Update Example

In the following figure, the controller and switches B and C form the Flexlink through a Flex Links pair. Port 3 is forwarding traffic, and port 4 is in the backup state. Switch A is an access switch, and ports 1 and 2 on switch A are connected to uplink switches B and C. The MAC addresses of the wireless clients have been learnt on port 1 of the switch A.



In the above figure, three wireless clients connect to an access point and communicate to the controller. The PC connected to switch A communicates with the wireless clients through the data path from port 3 to port 1. If the MAC address-table move update feature is not configured on the controller and port 3 goes down, port 4 starts forwarding traffic. However, for a short time the wireless clients will not be able to pass any traffic to the PC as port 3 is down.

If the MAC address-table move update feature is configured and enabled on the controller, and port 3 goes down, the controller sends a MAC address-table move update packet (MMU) from port 4. This MMU packet carries all the MAC addresses of the wireless clients. Switch C gets this packet on port 4 and immediately learns the MAC addresses of the wireless clients, which reduces the reconvergence time. The PC transmits data to the wireless clients using the path from port 2 to port 4. Switch C also bridges the same MMU packet in the VLAN so that all the switches in the network will update the MAC address table to ensure that the next packet to any wireless client towards controller comes on the right path. The controller learns only the MAC addresses of the wireless clients.

Related Topics

Configuring a Switch to Obtain and Process MAC Address-Table Move Update Messages (CLI), on page 187
Configuring MAC Address-Table Move Update (CLI), on page 186
Configuring the MAC Address-Table Move Update: Examples, on page 190

Flex Links VLAN Load Balancing Configuration Guidelines

- For Flex Links VLAN load balancing, you must choose the preferred VLANs on the backup interface.
- You cannot configure a preemption mechanism and VLAN load balancing for the same Flex Links pair.

Related Topics

Configuring VLAN Load Balancing on Flex Links (CLI), on page 185
Configuring VLAN Load Balancing on Flex Links: Examples, on page 189

MAC Address-Table Move Update Configuration Guidelines

- You can enable and configure this feature on the access switch to *send* the MAC address-table move updates.
- You can enable and configure this feature on the uplink switches to *get* the MAC address-table move updates.

Default Flex Links and MAC Address-Table Move Update Configuration

- Flex Links is not configured, and there are no backup interfaces defined.
- The preemption mode is off.
- The preemption delay is 35 seconds.
- The MAC address-table move update feature is not configured on the switch.

Related Topics

Configuring a Preemption Scheme for a Pair of Flex Links (CLI), on page 183
Configuring Flex Links (CLI), on page 182
Configuring Flex Links: Examples, on page 188

How to Configure Flex Links and the MAC Address-Table Move Update Feature

Configuring Flex Links (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(conf)# interface gigabitethernet1/0/1`	Specifies the interface, and enters interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface). The port-channel range is 1 to 128.
Step 3	**switchport backup interface** *interface-id* **Example:**	Configures a physical Layer 2 interface (or port channel) as part of a Flex Links pair with the

	Command or Action	Purpose
	`Switch(conf-if)# switchport backup interface gigabitethernet1/0/2`	interface. When one link is forwarding traffic, the other interface is in standby mode.
Step 4	**end** **Example:** `Switch(conf-if)# end`	Returns to privileged EXEC mode.

Related Topics

Flex Links, on page 176
Default Flex Links and MAC Address-Table Move Update Configuration, on page 182
Restrictions for Configuring Flex Links and MAC Address-Table Move Update, on page 175
Configuring Flex Links: Examples, on page 188
Flex Links Configuration, on page 177
Monitoring Flex Links, Multicast Fast Convergence, and MAC Address-Table Move Update, on page 188

Configuring a Preemption Scheme for a Pair of Flex Links (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode
Step 2	**interface** *interface-id* **Example:** `Switch(conf)# interface gigabitethernet1/0/1`	Specifies the interface, and enters interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface). The port-channel range is 1 to 128.
Step 3	**switchport backup interface** *interface-id* **Example:** `Switch(conf-if)# switchport backup interface gigabitethernet1/0/2`	Configures a physical Layer 2 interface (or port channel) as part of a Flex Links pair with the interface. When one link is forwarding traffic, the other interface is in standby mode.

	Command or Action	Purpose
Step 4	**switchport backup interface** *interface-id* **preemption mode** [**forced** | **bandwidth** | **off**] **Example:** `Switch(conf-if)# switchport backup interface gigabitethernet1/0/2 preemption mode forced`	Configures a preemption mechanism and delay for a Flex Links interface pair. You can configure the preemption as: • **forced**—(Optional) The active interface always preempts the backup. • **bandwidth**—(Optional) The interface with the higher bandwidth always acts as the active interface. • **off**—(Optional) No preemption occurs from active to backup.
Step 5	**switchport backup interface** *interface-id* **preemption delay** *delay-time* **Example:** `Switch(conf-if)# switchport backup interface gigabitethernet1/0/2 preemption delay 50`	Configures the time delay until a port preempts another port. **Note** Setting a delay time only works with forced and bandwidth modes.
Step 6	**end** **Example:** `Switch(conf-if)# end`	Returns to privileged EXEC mode.
Step 7	**show interface** [*interface-id*] **switchport backup** **Example:** `Switch# show interface gigabitethernet1/0/2 switchport backup`	Verifies the configuration.
Step 8	**copy running-config startup config** **Example:** `Switch# copy running-config startup config`	(Optional) Saves your entries in the switch startup configuration file.

Related Topics

Flex Links, on page 176
Default Flex Links and MAC Address-Table Move Update Configuration, on page 182
Restrictions for Configuring Flex Links and MAC Address-Table Move Update, on page 175
Configuring Flex Links: Examples, on page 188

Flex Links Configuration, on page 177
Monitoring Flex Links, Multicast Fast Convergence, and MAC Address-Table Move Update, on page 188

Configuring VLAN Load Balancing on Flex Links (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch (config)# interface gigabitethernet2/0/6`	Specifies the interface, and enters interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface). The port-channel range is 1 to 128.
Step 3	**switchport backup interface** *interface-id* **prefer vlan** *vlan-range* **Example:** `Switch (config-if)# switchport backup interface gigabitethernet2/0/8 prefer vlan 2`	Configures a physical Layer 2 interface (or port channel) as part of a Flex Links pair with the interface and specifies the VLANs carried on the interface. The VLAN ID range is 1 to 4094.
Step 4	**end** **Example:** `Switch (config-if)# end`	Returns to privileged EXEC mode.

Related Topics

Flex Links VLAN Load Balancing Configuration Guidelines, on page 181
Restrictions for Configuring Flex Links and MAC Address-Table Move Update, on page 175
Configuring VLAN Load Balancing on Flex Links: Examples, on page 189
Monitoring Flex Links, Multicast Fast Convergence, and MAC Address-Table Move Update, on page 188

Configuring MAC Address-Table Move Update (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch#interface gigabitethernet1/0/1`	Specifies the interface, and enters interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface). The port-channel range is 1 to 128.
Step 3	Use one of the following: • **switchport backup interface** *interface-id* • **switchport backup interface** *interface-id* **mmu primary vlan** *vlan-id* **Example:** `Switch(config-if)# switchport backup interface gigabitethernet0/2 mmu primary vlan 2`	Configures a physical Layer 2 interface (or port channel), as part of a Flex Links pair with the interface. The MAC address-table move update VLAN is the lowest VLAN ID on the interface. Configure a physical Layer 2 interface (or port channel) and specifies the VLAN ID on the interface, which is used for sending the MAC address-table move update. When one link is forwarding traffic, the other interface is in standby mode.
Step 4	**end** **Example:** `Switch(config-if)# end`	Returns to global configuration mode.
Step 5	**mac address-table move update transmit** **Example:** `Switch(config)# mac address-table move update transmit`	Enables the access switch to send MAC address-table move updates to other switches in the network if the primary link goes down and the switch starts forwarding traffic through the standby link. Enter command **mac address-table move update** on the switch, for MMU packets to update MAC tables. When the primary link comes back up, the MAC tables need to reconverge and this command will transmit the MMU, that will establish the behavior.
Step 6	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Switch(config)# end`	

Related Topics

Configuring the MAC Address-Table Move Update: Examples, on page 190
Monitoring Flex Links, Multicast Fast Convergence, and MAC Address-Table Move Update, on page 188
MAC Address-Table Move Update, on page 179
Restrictions for Configuring Flex Links and MAC Address-Table Move Update, on page 175

Configuring a Switch to Obtain and Process MAC Address-Table Move Update Messages (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode
Step 2	**mac address-table move update receive** **Example:** `Switch (config)# mac address-table move update receive`	Enables the switch to obtain and processes the MAC address-table move updates.
Step 3	**end** **Example:** `Switch (config)# end`	Returns to privileged EXEC mode.

Related Topics

Monitoring Flex Links, Multicast Fast Convergence, and MAC Address-Table Move Update, on page 188
Configuring the MAC Address-Table Move Update: Examples, on page 190
MAC Address-Table Move Update, on page 179
Restrictions for Configuring Flex Links and MAC Address-Table Move Update, on page 175

Monitoring Flex Links, Multicast Fast Convergence, and MAC Address-Table Move Update

Command	Purpose
show interface [*interface-id*] **switchport backup**	Displays the Flex Links backup interface configured for an interface or all the configured Flex Links and the state of each active and backup interface (up or standby mode).
show ip igmp profile address-table move update *profile-id*	Displays the specified IGMP profile or all the IGMP profiles defined on the switch.
show mac address-table move update	Displays the MAC address-table move update information on the switch.

Related Topics

Configuring a Preemption Scheme for a Pair of Flex Links (CLI), on page 183
Configuring Flex Links (CLI), on page 182

Configuration Examples for Flex Links

Configuring Flex Links: Examples

This example shows how to verify the configuration after you configure an interface with a backup interface:

```
Switch# show interface switchport backup

Switch Backup Interface Pairs:
Active Interface Backup Interface State
------------------------------------------------------------------------
GigabitEthernet1/0/1 GigabitEthernet1/0/2 Active Up/Backup Standby
```

This example shows how to verify the configuration after you configure the preemption mode as forced for a backup interface pair:

```
Switch# show interface switchport backup detail

Switch Backup Interface Pairs:

Active Interface Backup Interface State
------------------------------------------------------------------------
GigabitEthernet1/0/211 GigabitEthernet1/0/2 Active Up/Backup Standby
Interface Pair : Gi1/0/1, Gi1/0/2
Preemption Mode : forced
Preemption Delay : 50 seconds
Bandwidth : 100000 Kbit (Gi1/0/1), 100000 Kbit (Gi1/0/2)
Mac Address Move Update Vlan : auto
```

Related Topics

Configuring a Preemption Scheme for a Pair of Flex Links (CLI), on page 183
Configuring Flex Links (CLI), on page 182
Flex Links, on page 176
Default Flex Links and MAC Address-Table Move Update Configuration, on page 182
Restrictions for Configuring Flex Links and MAC Address-Table Move Update, on page 175

Configuring VLAN Load Balancing on Flex Links: Examples

In the following example, VLANs 1 to 50, 60, and 100 to 120 are configured on the switch:

```
Switch(config)# interface gigabitethernet 2/0/6
Switch(config-if)# switchport backup interface gigabitethernet 2/0/8 prefer vlan 60,100-120
```

When both interfaces are up, Gi2/0/8 forwards traffic for VLANs 60 and 100 to 120 and Gi2/0/6 forwards traffic for VLANs 1 to 50.

```
Switch# show interfaces switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet2/0/6    GigabitEthernet2/0/8    Active Up/Backup Standby

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

When a Flex Links interface goes down (LINK_DOWN), VLANs preferred on this interface are moved to the peer interface of the Flex Links pair. In this example, if interface Gi2/0/6 goes down, Gi2/0/8 carries all VLANs of the Flex Links pair.

```
Switch# show interfaces switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet2/0/6    GigabitEthernet2/0/8    Active Down/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

When a Flex Links interface comes up, VLANs preferred on this interface are blocked on the peer interface and moved to the forwarding state on the interface that has just come up. In this example, if interface Gi2/0/6 comes up, VLANs preferred on this interface are blocked on the peer interface Gi2/0/8 and forwarded on Gi2/0/6.

```
Switch# show interfaces switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
```

```
--------------------------------------------------------------------------
GigabitEthernet2/0/6    GigabitEthernet2/0/8    Active Up/Backup Standby

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120

Switch# show interfaces switchport backup detail

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
--------------------------------------------------------------------------
FastEthernet1/0/3       FastEthernet1/0/4       Active Down/Backup Up

Vlans Preferred on Active Interface: 1-2,5-4094
Vlans Preferred on Backup Interface: 3-4
Preemption Mode  : off
Bandwidth : 10000 Kbit (Fa1/0/3), 100000 Kbit (Fa1/0/4)
Mac Address Move Update Vlan : auto
```

Related Topics

Configuring VLAN Load Balancing on Flex Links (CLI), on page 185
Flex Links VLAN Load Balancing Configuration Guidelines, on page 181
Restrictions for Configuring Flex Links and MAC Address-Table Move Update, on page 175

Configuring the MAC Address-Table Move Update: Examples

This example shows how to verify the configuration after you configure an access switch to send MAC address-table move updates:

```
Switch# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 5
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 000b.462d.c502
Rcv last switch-ID : 0403.fd6a.8700
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

Related Topics

Configuring MAC Address-Table Move Update (CLI), on page 186
Configuring a Switch to Obtain and Process MAC Address-Table Move Update Messages (CLI), on page 187
MAC Address-Table Move Update, on page 179

Restrictions for Configuring Flex Links and MAC Address-Table Move Update, on page 175

Configuring Multicast Fast Convergence with Flex Links Failover: Examples

These are configuration examples for learning the other Flex Links port as the mrouter port when Flex Links is configured on GigabitEthernet1/0/11 and GigabitEthernet1/0/12, and output for the **show interfaces switchport backup** command:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet1/0/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport backup interface GigabitEthernet1/0/12
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet1/0/12
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# end
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface Backup Interface State
GigabitEthernet1/0/11 GigabitEthernet1/0/12 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : Off
Bandwidth : 100000 Kbit (Gi1/0/11), 100000 Kbit (Gi1/0/12)
Mac Address Move Update Vlan : auto
```

This output shows a querier for VLANs 1 and 401, with their queries reaching the switch through GigabitEthernet1/0/11:

```
Switch# show ip igmp snooping querier

Vlan   IP Address     IGMP Version      Port
-----------------------------------------------------------
1      1.1.1.1        v2      Gi1/0/11
401    41.41.41.1     v2      Gi1/0/11
```

This example is output for the **show ip igmp snooping mrouter** command for VLANs 1 and 401:

```
Switch# show ip igmp snooping mrouter

Vlan   ports
----   -----
1     Gi1/0/11(dynamic), Gi1/0/12(dynamic)
401   Gi1/0/11(dynamic), Gi1/0/12(dynamic)
```

Similarly, both Flex Links ports are part of learned groups. In this example, GigabitEthernet2/0/11 is a receiver/host in VLAN 1, which is interested in two multicast groups:

```
Switch# show ip igmp snooping groups

Vlan   Group    Type   Version    Port List
------------------------------------------------------------------------
1   228.1.5.1    igmp   v2    Gi1/0/11, Gi1/0/12, Gi2/0/11
```

```
1   228.1.5.2    igmp   v2    Gi1/0/11, Gi1/0/12, Gi2/0/11
```

When a host responds to the general query, the switch forwards this report on all the mrouter ports. In this example, when a host sends a report for the group 228.1.5.1, it is forwarded only on GigabitEthernet1/0/11, because the backup port GigabitEthernet1/0/12 is blocked. When the active link, GigabitEthernet1/0/11, goes down, the backup port, GigabitEthernet1/0/12, begins forwarding.

As soon as this port starts forwarding, the switch sends proxy reports for the groups 228.1.5.1 and 228.1.5.2 on behalf of the host. The upstream router learns the groups and starts forwarding multicast data. This is the default behavior of Flex Links. This behavior changes when the user configures fast convergence using the **switchport backup interface gigabitEthernet 1/0/12 multicast fast-convergence** command. This example shows turning on this feature:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitEthernet 1/0/11
Switch(config-if)# switchport backup interface gigabitEthernet 1/0/12 multicast
fast-convergence
Switch(config-if)# exit
Switch# show interfaces switchport backup detail

Switch Backup Interface Pairs:
Active       Interface       Backup Interface State
------------------------------------------------------------------------
GigabitEthernet1/0/11  GigabitEthernet1/0/12  Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : On
Bandwidth : 100000 Kbit (Gi1/0/11), 100000 Kbit (Gi1/0/12)
Mac Address Move Update Vlan : auto
```

This output shows a querier for VLAN 1 and 401 with their queries reaching the switch through GigabitEthernet1/0/11:

```
Switch# show ip igmp snooping querier

Vlan    IP Address     IGMP Version     Port
---------------------------------------------------------------
1      1.1.1.1        v2     Gi1/0/11
401    41.41.41.1     v2     Gi1/0/11
```

This is output for the **show ip igmp snooping mrouter** command for VLAN 1 and 401:

```
Switch# show ip igmp snooping mrouter

Vlan    ports
----    -----
1    Gi1/0/11(dynamic), Gi1/0/12(dynamic)
401    Gi1/0/11(dynamic), Gi1/0/12(dynamic)
```

Similarly, both the Flex Links ports are a part of the learned groups. In this example, GigabitEthernet2/0/11 is a receiver/host in VLAN 1, which is interested in two multicast groups:

```
Switch# show ip igmp snooping groups

Vlan   Group    Type   Version    Port List
------------------------------------------------------------------------
```

```
1    228.1.5.1     igmp    v2     Gi1/0/11, Gi1/0/12, Gi2/0/11
1    228.1.5.2     igmp    v2     Gi1/0/11, Gi1/0/12, Gi2/0/11
```

Whenever a host responds to the general query, the switch forwards this report on all the mrouter ports. When you turn on this feature through the command-line port, and when a report is forwarded by the switch on GigabitEthernet1/0/11, it is also leaked to the backup port GigabitEthernet1/0/12. The upstream router learns the groups and starts forwarding multicast data, which is dropped at the ingress because GigabitEthernet1/0/12 is blocked. When the active link, GigabitEthernet1/0/11, goes down, the backup port, GigabitEthernet1/0/12, begins forwarding. You do not need to send any proxy reports as the multicast data is already being forwarded by the upstream router. By leaking reports to the backup port, a redundant multicast path has been set up, and the time taken for the multicast traffic convergence is very minimal.

Related Topics

Multicast Fast Convergence with Flex Links Failover, on page 178

Additional References for Flex Links and MAC Address-Table Move Update

Related Documents

Related Topic	Document Title
Layer 2 command reference	*Layer 2/3 Command Reference (Catalyst 3850 Switches)Layer 2 Command Reference (Cisco WLC 5700 Series)*
switchport backup interface command	*Interface and Hardware Component Command Reference (Catalyst 3850 Switches)Interface Command Reference (Cisco WLC 5700 Series)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

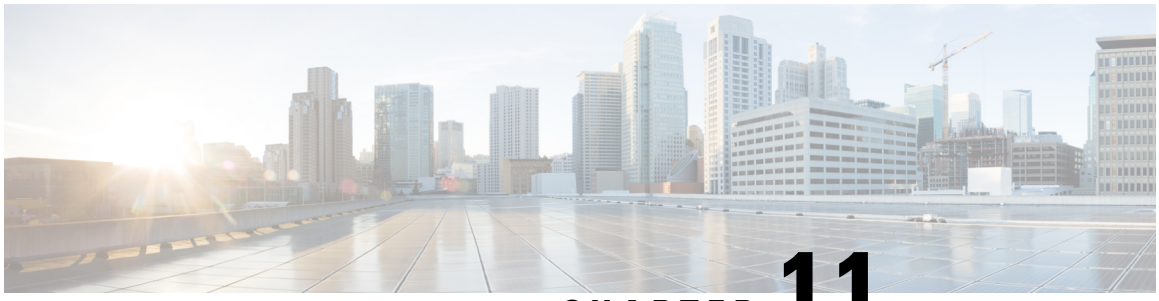
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Flex Links and MAC Address-Table Move Update

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.
Cisco IOS XE 3.3SE	Support for multicast fast convergence with Flex Links failover was added.



CHAPTER 11

Configuring UniDirectional Link Detection

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring UDLD

The following are restrictions for configuring UniDirectional Link Detection (UDLD):

- A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch.
- When configuring the mode (normal or aggressive), make sure that the same mode is configured on both sides of the link.
- You can configure UDLD in interface configuration mode and the configuration is accepted by the device; however, this configuration is not displayed in the running configuration, nor is it saved.

⚠

Caution Loop guard works only on point-to-point links. We recommend that each end of the link has a directly connected device that is running STP.

Information About UDLD

UniDirectional Link Detection (UDLD) is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. All connected devices must support UDLD for the protocol to successfully identify and disable unidirectional links. When UDLD detects a unidirectional link, it disables the affected port and alerts you. Unidirectional links can cause a variety of problems, including spanning-tree topology loops.

Modes of Operation

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD can detect unidirectional links due to misconnected ports on fiber-optic connections. In aggressive mode, UDLD can also detect unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and to misconnected ports on fiber-optic links.

In normal and aggressive modes, UDLD works with the Layer 1 mechanisms to learn the physical status of a link. At Layer 1, autonegotiation takes care of physical signaling and fault detection. UDLD performs tasks that autonegotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected ports. When you enable both autonegotiation and UDLD, the Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.

A unidirectional link occurs whenever traffic sent by a local device is received by its neighbor but traffic from the neighbor is not received by the local device.

Normal Mode

In normal mode, UDLD detects a unidirectional link when fiber strands in a fiber-optic port are misconnected and the Layer 1 mechanisms do not detect this misconnection. If the ports are connected correctly but the traffic is one way, UDLD does not detect the unidirectional link because the Layer 1 mechanism, which is supposed to detect this condition, does not do so. In this case, the logical link is considered undetermined, and UDLD does not disable the port.

When UDLD is in normal mode, if one of the fiber strands in a pair is disconnected, as long as autonegotiation is active, the link does not stay up because the Layer 1 mechanisms detects a physical problem with the link. In this case, UDLD does not take any action and the logical link is considered undetermined.

Related Topics

Enabling UDLD Globally (CLI), on page 199
Enabling UDLD on an Interface (CLI), on page 200

Aggressive Mode

In aggressive mode, UDLD detects a unidirectional link by using the previous detection methods. UDLD in aggressive mode can also detect a unidirectional link on a point-to-point link on which no failure between the two devices is allowed. It can also detect a unidirectional link when one of these problems exists:

- On fiber-optic or twisted-pair links, one of the ports cannot send or receive traffic.
- On fiber-optic or twisted-pair links, one of the ports is down while the other is up.
- One of the fiber strands in the cable is disconnected.

In these cases, UDLD disables the affected port.

In a point-to-point link, UDLD hello packets can be considered as a heart beat whose presence guarantees the health of the link. Conversely, the loss of the heart beat means that the link must be shut down if it is not possible to reestablish a bidirectional link.

If both fiber strands in a cable are working normally from a Layer 1 perspective, UDLD in aggressive mode detects whether those fiber strands are connected correctly and whether traffic is flowing bidirectionally between the correct neighbors. This check cannot be performed by autonegotiation because autonegotiation operates at Layer 1.

Note Udld is enabled with udld aggressive mode globally. When Rx cable or Tx is cable from switch1 , then the switch1 and switch2 ports will go into **Not connected** state. They do not go to **error disabled** state. Also the port does not show any light if you check the physical connection.

Switch1 (Tx)_____(Rx) Switch2

Switch1 (Rx)_____(Tx) Switch2

Related Topics

Enabling UDLD Globally (CLI), on page 199
Enabling UDLD on an Interface (CLI), on page 200

Methods to Detect Unidirectional Links

UDLD operates by using two methods:

- Neighbor database maintenance
- Event-driven detection and echoing

Related Topics

Enabling UDLD Globally (CLI), on page 199
Enabling UDLD on an Interface (CLI), on page 200

Neighbor Database Maintenance

UDLD learns about other UDLD-capable neighbors by periodically sending a hello packet (also called an advertisement or probe) on every active port to keep each device informed about its neighbors.

When the switch receives a hello message, it caches the information until the age time (hold time or time-to-live) expires. If the switch receives a new hello message before an older cache entry ages, the switch replaces the older entry with the new one.

Whenever a port is disabled and UDLD is running, whenever UDLD is disabled on a port, or whenever the switch is reset, UDLD clears all existing cache entries for the ports affected by the configuration change. UDLD sends at least one message to inform the neighbors to flush the part of their caches affected by the status change. The message is intended to keep the caches synchronized.

Event-Driven Detection and Echoing

UDLD relies on echoing as its detection operation. Whenever a UDLD device learns about a new neighbor or receives a resynchronization request from an out-of-sync neighbor, it restarts the detection window on its side of the connection and sends echo messages in reply. Because this behavior is the same on all UDLD neighbors, the sender of the echoes expects to receive an echo in reply.

If the detection window ends and no valid reply message is received, the link might shut down, depending on the UDLD mode. When UDLD is in normal mode, the link might be considered undetermined and might not be shut down. When UDLD is in aggressive mode, the link is considered unidirectional, and the port is disabled.

Related Topics

Enabling UDLD Globally (CLI), on page 199
Enabling UDLD on an Interface (CLI), on page 200

UDLD Reset Options

If an interface becomes disabled by UDLD, you can use one of the following options to reset UDLD:

- The **udld reset** interface configuration command.
- The **shutdown** interface configuration command followed by the **no shutdown** interface configuration command restarts the disabled port.
- The **no udld** {**aggressive** | **enable**} global configuration command followed by the **udld** {**aggressive** | **enable**} global configuration command reenables the disabled ports.
- The **no udld port** interface configuration command followed by the **udld port** [**aggressive**] interface configuration command reenables the disabled fiber-optic port.
- The **errdisable recovery cause udld** global configuration command enables the timer to automatically recover from the UDLD error-disabled state, and the **errdisable recovery interval** *interval* global configuration command specifies the time to recover from the UDLD error-disabled state.

Related Topics

Enabling UDLD Globally (CLI), on page 199
Enabling UDLD on an Interface (CLI), on page 200

Default UDLD Configuration

Table 11: Default UDLD Configuration

Feature	Default Setting
UDLD global enable state	Globally disabled
UDLD per-port enable state for fiber-optic media	Disabled on all Ethernet fiber-optic ports
UDLD per-port enable state for twisted-pair (copper) media	Disabled on all Ethernet 10/100 and 1000BASE-TX ports
UDLD aggressive mode	Disabled

Related Topics

Enabling UDLD Globally (CLI), on page 199
Enabling UDLD on an Interface (CLI), on page 200

How to Configure UDLD

Enabling UDLD Globally (CLI)

Follow these steps to enable UDLD in the aggressive or normal mode and to set the configurable message timer on all fiber-optic ports on the switch.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 2	**udld** {**aggressive** | **enable** | **message time** *message-timer-interval*}
	Example:
	`Switch(config)# udld enable`
	`message time 10`
		Specifies the UDLD mode of operation:
		• **aggressive**—Enables UDLD in aggressive mode on all fiber-optic ports.
		• **enable**—Enables UDLD in normal mode on all fiber-optic ports on the switch. UDLD is disabled by default.
		An individual interface configuration overrides the setting of the **udld enable** global configuration command.
		• **message time** *message-timer-interval*—Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are detected to be bidirectional. The range is from 1 to 90 seconds; the default value is 15.
		Note This command affects fiber-optic ports only. Use the **udld** interface configuration command to enable UDLD on other port types.
		Use the **no** form of this command, to disable UDLD.

	Command or Action	Purpose
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Related Topics

Monitoring and Maintaining UDLD
Aggressive Mode, on page 196
Normal Mode, on page 196
Methods to Detect Unidirectional Links, on page 197
Event-Driven Detection and Echoing, on page 198
UDLD Reset Options, on page 198
Default UDLD Configuration, on page 198

Enabling UDLD on an Interface (CLI)

Follow these steps either to enable UDLD in the aggressive or normal mode or to disable UDLD on a port.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Specifies the port to be enabled for UDLD, and enters interface configuration mode.
Step 3	**udld port** [**aggressive**] **Example:** `Switch(config-if)# udld port aggressive`	UDLD is disabled by default. • **udld port**—Enables UDLD in normal mode on the specified port. • **udld port aggressive**—(Optional) Enables UDLD in aggressive mode on the specified port.

	Command or Action	Purpose
		Note Use the **no udld port** interface configuration command to disable UDLD on a specified fiber-optic port.
Step 4	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Related Topics

Monitoring and Maintaing UDLD
Aggressive Mode, on page 196
Normal Mode, on page 196
Methods to Detect Unidirectional Links, on page 197
Event-Driven Detection and Echoing, on page 198
UDLD Reset Options, on page 198
Default UDLD Configuration, on page 198

Monitoring and Maintaining UDLD

Command	Purpose
show udld [*interface-id* | **neighbors**]	Displays the UDLD status for the specified port or for all ports.

Additional References for UDLD

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	*Layer 2/3 Command Reference (Catalyst 3850 Switches)Layer 2 Command Reference (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

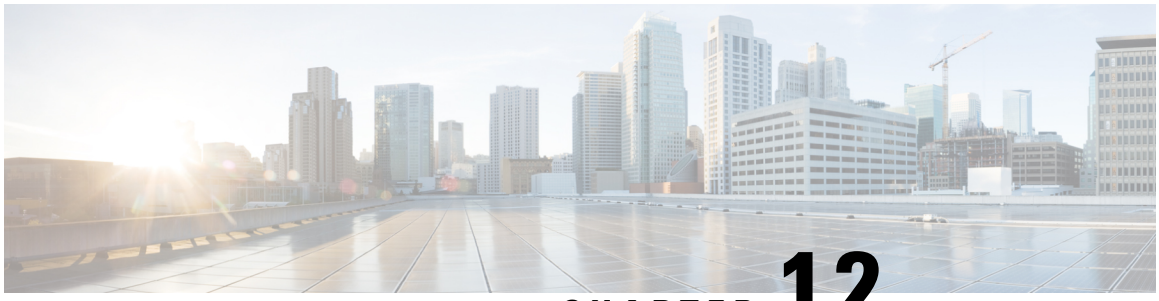
Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for UDLD

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.

PART V

Lightweight Access Point



CHAPTER 12

Configuring the Switch for Access Point Discovery

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring the Switch for Access Point Discovery

⚠

Caution You should connect APs directly to the Cisco Catalyst 3850 switch ports to use its wireless functionality.

- Ensure that the Control and Provisioning of Wireless Access Points (CAPWAP) UDP ports 5246 and 5247 (similar to the Lightweight Access Point Protocol (LWAPP) UDP ports 12222 and 12223) are enabled and are not blocked by an intermediate device that could prevent an access point from joining the switch.
- If access control lists (ACLs) are in the control path between the switch and its access points, you must open new protocol ports to prevent access points from being stranded.

- If an access point is in the UP state and its IP address changes, the access point tears down the existing CAPWAP tunnel and rejoins the switch.
- Access points must be discovered by a switch before they can become an active part of the network. The lightweight access points support the following switch discovery processes:
  - Layer 3 CAPWAP discovery—You can enable this feature on different subnets from the access point. This feature uses IP addresses and UDP packets rather the MAC addresses used by Layer 2 discovery.
  - Locally stored switch IP address discovery—If the access point was previously associated to a switch, the IP addresses of the primary, secondary, and tertiary switchs are stored in the access point's nonvolatile memory. This process of storing switch IP addresses on an access point for later deployment is called *priming the access point*.
  - DHCP server discovery—This feature uses DHCP option 43 to provide switch IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability.
  - DNS discovery—The access point can discover switchs through your domain name server (DNS). You must configure your DNS to return switch IP addresses in response to CISCO-CAPWAP-CONTROLLER.*localdomain*, where *localdomain* is the access point domain name. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.*localdomain*. When the DNS sends a list of switch IP addresses, the access point sends discovery requests to the switchs.

Restrictions for Configuring the Switch for Access Point Discovery

- Ensure that the switchs are configured with the correct date and time. If the date and time configured on the switch precedes the creation and installation date of certificates on the access points, the access point fails to join the switch.
- During the discovery process, access points that are supported by the Cisco switch, such as the 1140, 1260, 3500, 1040,1600, 2600, or 3600 query only for Cisco switchs.
- Do not configure same VLAN for both wireless management and wireless clients.

Information About Configuring the Switch for Access Point Discovery

In a CAPWAP environment, a lightweight access point discovers a switch by using CAPWAP discovery mechanisms and then sends a CAPWAP join request to the switch. The switch sends a CAPWAP join response to the access point that allows the access point to join the switch. When the access point joins the switch, the switch manages its configuration, firmware, control transactions, and data transactions.

Access Point Communication Protocols

Cisco lightweight access points use the IETF standard CAPWAP to communicate with the switch and other lightweight access points on the network.

CAPWAP, which is based on LWAPP, is a standard, interoperable protocol that enables a switch to manage a collection of wireless access points. CAPWAP is implemented in switch for these reasons:

- To provide an upgrade path from Cisco products that use LWAPP to next-generation Cisco products that use CAPWAP
- To manage RFID readers and similar devices
- To enable switchs to interoperate with third-party access points in the future

Viewing Access Point Join Information

Join statistics for an access point that sends a CAPWAP discovery request to the switch at least once are maintained on the switch even if the access point is rebooted or disconnected. These statistics are removed only when the switch is rebooted or when you choose to clear the statistics.

Troubleshooting the Access Point Join Process

Access points can fail to join a switch for many reasons such as a RADIUS authorization is pending, self-signed certificates are not enabled on the switch, the access point and switch's regulatory domains do not match, and so on.

You can configure the access points to send all CAPWAP-related errors to a syslog server. You do not need to enable any debug commands on the switch because all of the CAPWAP error messages can be viewed from the syslog server itself.

The state of the access point is not maintained on the switch until it receives a CAPWAP join request from the access point, so it can be difficult to determine why the CAPWAP discovery request from a certain access point was rejected. In order to troubleshoot such joining issues without enabling CAPWAP debug commands on the switch, the switch collects information for all access points that send a discovery message to this switch and maintains information for any access points that have successfully joined this switch.

The switch collects all join-related information for each access point that sends a CAPWAP discovery request to the switch. Collection begins when the first discovery message is received from the access point and ends when the last configuration payload is sent from the switch to the access point.

When the switch is maintaining join-related information for the maximum number of access points, it does not collect information for any more access points.

You can also configure a DHCP server to return a syslog server IP address to the access point using option 7 on the server. The access point then starts sending all syslog messages to this IP address.

You can configure the syslog server IP address through the access point CLI, if the access point is not connected to the switch by entering the **capwap ap log-server** *syslog_server_IP_address* command.

When the access point joins a switch for the first time, the switch pushes the global syslog server IP address (the default is 255.255.255.255) to the access point. After that, the access point sends all syslog messages to this IP address, until it is overridden by one of the following scenarios:

- The access point is still connected to the same switch, and you changed the global syslog server IP address configuration on the switch by using the **ap syslog host** *Syslog_Server_IP_Address* command. In this case, the switch pushes the new global syslog server IP address to the access point.
- The access point is still connected to the same switch, and you configured a specific syslog server IP address for the access point on the switch by using the **ap name** *Cisco_AP* **syslog host** *Syslog_Host_IP_Address* command. In this case, the switch pushes the new specific syslog server IP address to the access point.
- The access point gets disconnected from the switch, and you configured the syslog server IP address from the access point CLI by using the **capwap ap log-server** *syslog_server_IP_address* command. This command works only if the access point is not connected to any switch.
- The access point gets disconnected from the switch and joins another switch. In this case, the new switch pushes its global syslog server IP address to the access point.

Whenever a new syslog server IP address overrides the existing syslog server IP address, the old address is erased from persistent storage, and the new address is stored in its place. The access point also starts sending all syslog messages to the new IP address, if the access point can reach the syslog server IP address.

How to Configure Access Point Discovery

Configuring the Syslog Server for Access Points (CLI)

Procedure

	Command or Action	Purpose
Step 1	**show ap config global** **Example:** `Switch# show ap config global`	Displays the global syslog server settings for all access points that join the switch.
Step 2	**show ap name** *Cisco_AP* **config general** **Example:** `Switch# show ap name AP03 config general`	Displays the syslog server settings for a specific access point.

Monitoring Access Point Join Information (CLI)

Note The procedure to perform this task using the switch GUI is not currently available.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**show ap join stats summary** **Example:** `Switch# show ap join stats summary`	Displays the MAC addresses of all the access points that are joined to the switch or that have tried to join.
Step 3	**show ap mac-address** *mac_address* **join stats summary** **Example:** `Switch# show ap mac-address 000.2000.0400 join stats summary`	Displays all the statistics for the AP including the last join error detail.
Step 4	**show ap mac-address** *mac_address* **join stats detailed** **Example:** `Switch# show ap mac-address 000.2000.0400 join stats detailed`	Displays all join-related statistics collected for a specific access point.
Step 5	**clear ap join statistics** **Example:** `Switch# clear ap join statistics`	Clears the join statistics for all access points. **Note** To clear the join statistics that correspond to specific access points, enter the **clear ap mac-address** *mac_address* **join statistics** command.

Related Topics

Displaying the MAC Addresses of all Access Points: Example, on page 209
DHCP Option 43 for Lightweight Cisco Aironet Access Points Configuration Example, on page 211

Configuration Examples for Configuring the Switch for Access Point Discovery

Displaying the MAC Addresses of all Access Points: Example

This example shows how to display MAC addresses of all the access points that are joined to the switch:

```
Switch# show ap join stats summary
Number of APs.................................... 4

Base Mac          EthernetMac       AP Name IP Address    Status
----------------- ----------------- ------- ------------- ----------
```

```
00:0b:85:57:bc:c0 00:0b:85:57:bc:c0 AP1130  10.10.163.217 Joined
00:1c:0f:81:db:80 00:1c:63:23:ac:a0 AP1140  10.10.163.216 Not joined
00:1c:0f:81:fc:20 00:1b:d5:9f:7d:b2 AP1     10.10.163.215 Joined
00:21:1b:ea:36:60 00:0c:d4:8a:6b:c1 AP2     10.10.163.214 Not joined
```

This example shows how to display the last join error details for a specific access point:

```
Switch# show ap mac-address 000.2000.0400 join stats summary
Is the AP currently connected to controller..... Yes
Time at which the AP joined this
controller last time..... Aug 21 12:50:36.061
Type of error
that occurred last..... AP got or has been disconnected
Reason for error
that occurred last..... The AP has been reset by the controller
Time at which the last join error occurred..... Aug 21 12:50:34.374
```

This example shows how to display all join-related statistics collected for a specific access point:

```
Switch# show ap mac-address 000.2000.0400 join stats detailed
Discovery phase statistics
- Discovery requests received..... 2
- Successful discovery responses sent..... 2
- Unsuccessful discovery request processing..... 0
- Reason for last unsuccessful discovery attempt..... Not applicable
- Time at last successful discovery attempt..... Aug 21 12:50:23.335
- Time at last unsuccessful discovery attempt..... Not applicable

Join phase statistics
- Join requests received..... 1
- Successful join responses sent..... 1
- Unsuccessful join request processing..... 1
- Reason for last unsuccessful join attempt.....      RADIUS authorization
                                                      is pending
                                                      for the AP
- Time at last successful join attempt..... Aug 21 12:50:34.481
- Time at last unsuccessful join attempt..... Aug 21 12:50:34.374

Configuration phase statistics
- Configuration requests received..... 1
- Successful configuration responses sent..... 1
- Unsuccessful configuration request processing..... 0
- Reason for last unsuccessful configuration attempt.. Not applicable
- Time at last successful configuration attempt..... Aug 21 12:50:34.374
- Time at last unsuccessful configuration attempt..... Not applicable

Last AP message decryption failure details
- Reason for last message decryption failure..... Not applicable

Last AP disconnect details
- Reason for last AP connection failure..... The AP has been reset by
                                                      the controller
Last join error summary
- Type of error that occurred last..... AP got or has been
                                                      disconnected
- Reason for error that occurred last..... The AP has been reset
                                                      by the controller
- Time at which the last join error occurred..... Aug 21 12:50:34.374
```

DHCP Option 43 for Lightweight Cisco Aironet Access Points Configuration Example

For more information about the AP join process, see *DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration Example*.

Configuring AP Pass Through

Information About AP Pass Through

AP pass through allows all the access points connected to Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches to join another controller on the network.

Prior to this release, all access points connected Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches would be terminated on the switch when the wireless management vlan is turned on. Unsupported access points connected to the switch were unable join a controller on a different vlan. AP pass through allows the connected AP to join another wireless controller on the network by assigning different vlan.

The advantages of AP pass through are:

- Allows partial deployment of Cisco New Generation Wireless Controllers where some APs are connected to Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches but other APs continue to join other controllers on the network.
- The APs that are not supported on the Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches are allowed to join other controllers on the network.
- The wireless LAN controller is used to provide access to both wired and wireless guests. AP Pass through allows the AP to pass through Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches to join any other controller when wired guest accessing is turned on.

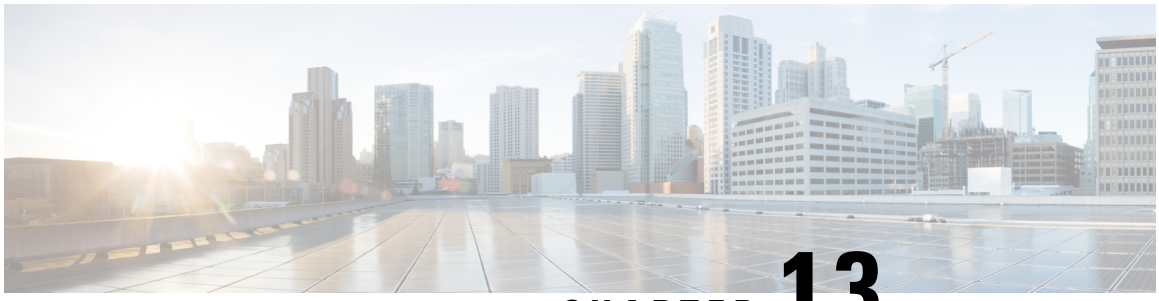
Configuring AP Pass Through

All access points on VLANs other than the one with supported access points will be put into the AP pass-through mode and will not terminate on theSwitch.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wireless management interface vlan** *vlan_id* **Example:**	Configures the ports that are connected to the supported access points with the wireless management VLAN

	Command or Action	Purpose
	`Switch(config)# wireless management interface vlan10`	
Step 3	**interface GigabitEthernet1/0/1** **Example:** `Switch(config)# interface TenGigabitEthernet1/0/1`	Sets the 10-Gigbit Ethernet interface. The command prompt changes from (config)# to (config-if)#.
Step 4	**description Supported AP switchport access** *vlan_id* **Example:** `Switch(config-if)# switchport access vlan10`	Specifies the VLAN for which this access port will carry traffic
Step 5	**description Unsupported AP switchport access** *vlan_id* **Example:** `Switch(config-if)# switchport access vlan20`	Configures the ports that are connected to the unsupported access points with a vlan other than the wireless management VLAN.



CHAPTER 13

Configuring Data Encryption

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Data Encryption

- Cisco 1260, 3500, 3600, 801, 1140, 1310, and 1520 series access points support Datagram Transport Layer Security (DTLS) data encryption.
- You can use the switch to enable or disable DTLS data encryption for a specific access point or for all access points.
- Non-Russian customers who use the Cisco switch do not need a data DTLS license.

Restrictions for Configuring Data Encryption

- Encryption limits throughput at both the switch and the access point, and maximum throughput is desired for most enterprise networks.
- If your switch does not have a data DTLS license and if the access point associated with the switch has DTLS enabled, the data path will be unencrypted.

- In images that do not have a DTLS license, the DTLS commands are not available.

Information About Data Encryption

The switch enables you to encrypt Control and Provisioning of Wireless Access Points (CAPWAP) control packets (and optionally, CAPWAP data packets) that are sent between the access point and the switch using DTLS. DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS. CAPWAP control packets are management packets exchanged between a switch and an access point while CAPWAP data packets encapsulate forwarded wireless frames. CAPWAP control and data packets are sent over separate UDP ports: 5246 (control) and 5247 (data). If an access point does not support DTLS data encryption, DTLS is enabled only for the control plane, and a DTLS session for the data plane is not established.

How to Configure Data Encryption

Configuring Data Encryption (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap link-encryption** **Example:** `Switch(config)# ap link-encryption`	Enables data encryption for all access points or a specific access point by entering this command. The default value is disabled. Changing the data encryption mode requires the access points to rejoin the switch.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 4	**show ap link-encryption** **Example:** `Switch# show ap link-encryption`	Displays the encryption state of all access points or a specific access point. This command also shows authentication errors, which track the number of integrity check failures and replay errors. Relay errors help in tracking the number of times the access point receives the same packet.
Step 5	**show wireless dtls connections** **Example:**	Displays a summary of all active DTLS connections.

	Command or Action	Purpose
	`Switch# show wireless dtls connections`	**Note** If you experience any problems with DTLS data encryption, enter the **debug dtls ap {all | event | trace}** command to debug all DTLS messages, events, or traces.

Related Topics

Displaying Data Encryption States for all Access Points: Examples, on page 215

Configuring Data Encryption (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points** > **All APs**.

The All APs page is displayed.

Step 2 Click the name of the access point for which you want to enable data encryption.

The **AP > Edit** page is displayed.

Step 3 Click the **Advanced** tab.

Step 4 Select or unselect the **Data Encryption** check box.

Note Changing the data encryption mode requires the access points to reassociate with the switch.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Configuration Examples for Configuring Data Encryption

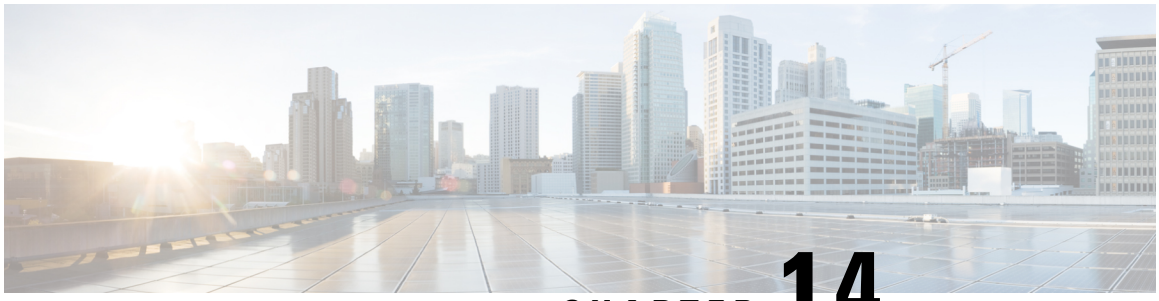
Displaying Data Encryption States for all Access Points: Examples

This example shows how to display the encryption state of all access points or a specific access point. This command also shows authentication errors, which track the number of integrity check failures and replay errors. Relay errors help in tracking the number of times the access point receives the same packet:

```
Switch# show ap link-encryption
                    Encryption  Dnstream  Upstream    Last
AP Name                  State     Count     Count  Update
------------------  ----------  --------  --------  ------
3602a                  Enabled         0         0   Never
```

This example shows how to display a summary of all active DTLS connections:

```
Switch# show wireless dtls connections
AP Name         Local Port   Peer IP       Peer Port  Ciphersuite
--------------- ------------ ------------- ---------- --------------------
3602a           Capwap_Ctrl  10.10.21.213  46075      TLS_RSA_WITH_AES_128_CBC_SHA
3602a           Capwap_Data  10.10.21.213  46075      TLS_RSA_WITH_AES_128_CBC_SHA
```



CHAPTER 14

Configuring Retransmission Interval and Retry Count

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring the Access Point Retransmission Interval and Retry Count

- You can configure the retransmission intervals and retry count both at a global and a specific access point level. A global configuration applies these configuration parameters to all the access points. Alternatively, when you configure the retransmission level and retry count at a specific access point level, the values are applied to that particular access point. The access point specific configuration has a higher precedence than the global configuration.

Information About Retransmission Interval and Retry Count

The switch and the access points exchange packets using the Control and Provisioning of Wireless Access Points (CAPWAP) reliable transport protocol. For each request, a response is defined. This response is used to acknowledge the receipt of the request message. Response messages are not explicitly acknowledged; therefore, if a response message is not received, the original request message is retransmitted after the retransmit interval. If the request is not acknowledged after a maximum number of retransmissions, the session is closed and the access points reassociate with another switch.

How to Configure Access Point Retransmission Interval and Retry Count

Configuring the Access Point Retransmission Interval and Retry Count (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ap capwap retransmit interval** *interval_time* **Example:** `Switch(config)# ap capwap retransmit interval 2`	Configures the control packet retransmit interval for all access points globally. **Note** The range for the interval parameter is from 2 to 5.
Step 4	**ap capwap retransmit count** *count_value* **Example:** `Switch(config)# ap capwap retransmit count 3`	Configures the control packet retry count for all access points globally. **Note** The range for the count is from 3 to 8.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 6	**ap name** *Cisco_AP* **capwap retransmit interval** *interval_time*	Configures the control packet retransmit interval for the individual access point that you specify.

	Command or Action	Purpose
	Example: `Switch# ap name AP02 capwap retransmit interval 2`	**Note** The range for the interval is from 2 to 5. **Note** You must be in privileged EXEC mode to use the **ap name** commands.
Step 7	**ap name** *Cisco_AP* **capwap retransmit count** *count_value* **Example:** `Switch# ap name AP02 capwap retransmit count 3`	Configures the control packet retry count for the individual access point that you specify. **Note** The range for the retry count is from 3 to 8.
Step 8	**show ap capwap retransmit** **Example:** `Switch# show ap capwap retransmit`	Displays the CAPWAP retransmit details.

Configuring the Access Point Retransmission Interval and Retry Count (GUI)

Procedure

- Global configuration applicable to all APs:
  a) Choose **Configuration** > **Wireless** > **Access Points** > **Global AP Configuration**.

     The **Global Configuration** page is displayed.

  b) In the **AP Retransmit Config Parameters** area, enter the values for the following parameters:

     - **AP Retransmit Count**—Number of times you want the access point to retransmit the request to the switch. The valid range is between 3 and 8.
     - **AP Retransmit Interval**—Duration between the retransmission of requests. The valid range is between 2 and 5.

  c) Click **Apply**.
  d) Click **Save Configuration**.
- Configuration that is applicable to a specific AP:
  a) Choose **Configuration** > **Wireless** > **Access Points** > **All APs**.

     The **All APs** page is displayed with a list of access points.

  b) Click the access point name.

     The **AP > Edit** page is displayed.

  c) Click the **Advanced** tab.
  d) In the **AP Retransmit Config Parameters** area, enter the values for the following **AP Retransmit Count** and **AP Retransmit Interval** parameters:

- **AP Retransmit Count**—Number of times you want the access point to retransmit the request to the switch. The valid range is between 3 and 8.
- **AP Retransmit Interval**—Duration between the retransmission of requests. The valid range is between 2 and 5.

e) Click **Apply**.
f) Click **Save Configuration**.

Viewing CAPWAP Maximum Transmission Unit Information (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**show ap name** *Cisco_AP* **config general** **Example:** `Switch# show ap name Maria-1250 config general | include MTU`	Displays the maximum transmission unit (MTU) for the CAPWAP path on the switch. The MTU specifies the maximum size of any packet (in bytes) in a transmission.

Related Topics

Viewing the CAPWAP Retransmission Details: Example, on page 221
Viewing Maximum Transmission Unit Information: Example, on page 221

Viewing CAPWAP Maximum Transmission Unit Information (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points** > **All APs**.

The **All APs** page is displayed.

Step 2 Click the AP name.

The **AP > Edit** page is displayed.

Step 3 Click the **Advanced** tab.

The **CAPWAP MTU** field shows the CAPWAP maximum retransmission unit information.

Configuration Examples for Configuring Access Point Retransmission Interval and Retry Count

Viewing the CAPWAP Retransmission Details: Example

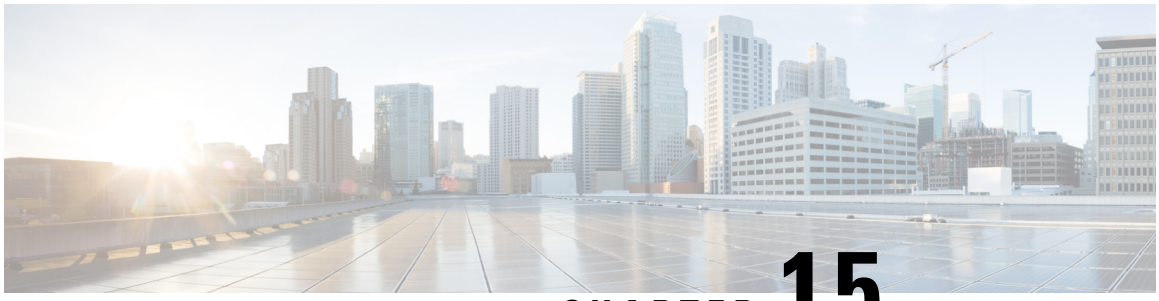
Enter the following command:

```
Switch# show ap capwap retransmit
Global control packet retransmit interval : 3
Global control packet retransmit count : 5

AP Name                          Retransmit Interval             Retransmit Count

-------------------------------- --------------------------------
--------------------------------
3602a                            5                               3
```

Viewing Maximum Transmission Unit Information: Example

This example shows how to view the maximum transmission unit (MTU) for the CAPWAP path on the switch. The MTU specifies the maximum size of any packet (in bytes) in a transmission:

```
Switch# show ap name cisco-ap-name config general | include MTU
CAPWAP Path MTU.................................. 1500
```



CHAPTER 15

Configuring Adaptive Wireless Intrusion Prevention System

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring wIPS

- The regular local mode access point has been extended with a subset of Wireless Intrusion Prevention System (wIPS) capabilities. This feature enables you to deploy your access points to provide protection without needing a separate overlay network.

How to Configure wIPS on Access Points

Configuring wIPS on an Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap name** *Cisco_AP* **mode local** **Example:** `Switch# ap name AP01 mode local`	Configures an access point for monitor mode. A message appears that indicates that changing the AP's mode causes the access point to reboot. This message also displays a prompt that enables you to specify whether or not you want to continue with changing the AP mode. Enter **y** at the prompt to continue.
Step 2	**ap name** *Cisco_AP* **dot11 5ghz shutdown** **Example:** `Switch# ap name AP01 dot11 5ghz shutdown`	Disables the 802.11a radio on the access point.
Step 3	**ap name** *Cisco_AP* **dot11 24ghz shutdown** **Example:** `Switch# ap name AP02 dot11 24ghz shutdown`	Disables the 802.11b radio on the access point.
Step 4	**ap name** *Cisco_AP* **mode monitor submode wips** **Example:** `Switch# ap name AP01 mode monitor submode wips`	Configures the wIPS submode on the access point. **Note** To disable wIPS on the access point, enter the **ap name** *Cisco_AP* **modemonitor submode none** command.
Step 5	**ap name** *Cisco_AP* **monitor-mode wips-optimized** **Example:** `Switch# ap name AP01 monitor-mode wips-optimized`	Enables wIPS optimized channel scanning for the access point. The access point scans each channel for 250 milliseconds. It derives the list of channels to be scanned from the monitor configuration. You can choose the following options: • **All**—All channels supported by the access point's radio. • **Country**—Only the channels supported by the access point's country of operation. • **DCA**—Only the channel set used by the dynamic channel assignment (DCA)

	Command or Action	Purpose
		algorithm, which by default includes all of the nonoverlapping channels allowed in the access point's country of operation.
Step 6	**show ap dot11 24ghz monitor** **Example:** `Switch# show ap dot11 24ghz monitor`	Displays the monitor configuration channel set. **Note** The 802.11b Monitor Channels value in the output of the command indicates the monitor configuration channel set.
Step 7	**ap name** *Cisco_AP* **no dot11 5ghz shutdown** **Example:** `Switch# ap name AP01 no dot11 5ghz shutdown`	Enables the 802.11a radio on the access point.
Step 8	**ap name** *Cisco_AP* **no dot11 24ghz shutdown** **Example:** `Switch# ap name AP01 no dot11 24ghz shutdown`	Enables the 802.11b radio on the access point.

Configuring wIPS on an Access Point (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points** > **All APs**

The **All APs** page is displayed.

Step 2 Click the access point name.

The **AP > Edit** page is displayed.

Step 3 From the **AP Mode** drop-down list, choose one of the following options to configure the AP mode parameters:

- **Local**
- **Monitor**

Step 4 From the **AP Sub Mode** drop-down list, choose **WIPS**.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Monitoring wIPS Information

Note The procedure to perform this task using the switch GUI is not currently available.

Procedure

	Command or Action	Purpose
Step 1	**show ap name** *Cisco_AP* **config general** **Example:** `Switch# show ap name AP01 config general`	Displays information on the wIPS submode on the access point.
Step 2	**show ap monitor-mode summary** **Example:** `Switch# show ap monitor-mode summary`	Displays the wIPS optimized channel scanning configuration on the access point.
Step 3	**show wireless wps wips summary** **Example:** `Switch# show wireless wps wips summary`	Displays the wIPS configuration forwarded by NCS or Prime to the switch.
Step 4	**show wireless wps wips statistics** **Example:** `Switch# show wireless wps wips statistics`	Displays the current state of wIPS operation on the switch.
Step 5	**clear wireless wips statistics** **Example:** `Switch# clear wireless wips statistics`	Clears the wIPS statistics on the switch.

Related Topics

Displaying the Monitor Configuration Channel Set: Example, on page 226
Displaying wIPS Information: Examples, on page 227

Configuration Examples for Configuring wIPS on Access Points

Displaying the Monitor Configuration Channel Set: Example

This example shows how to display the monitor configuration channel set:

```
Switch# show ap dot11 24ghz monitor
Default 802.11b AP monitoring
802.11b Monitor Mode.......................... enable
802.11b Monitor Channels...................... Country channels
802.11b AP Coverage Interval.................. 180 seconds
```

```
802.11b AP Load Interval..................... 60 seconds
802.11b AP Noise Interval..................... 180 seconds
802.11b AP Signal Strength Interval............ 60 seconds
```

Displaying wIPS Information: Examples

This example shows how to display information on the wIPS submode on the access point:

```
Switch# show ap name AP01 config general
Cisco AP Identifier.............. 3
Cisco AP Name.................... AP1131:46f2.98ac
...
AP Mode ......................... Monitor
Public Safety ................... Disabled Disabled
AP SubMode ...................... WIPS
```

This example shows how to display the wIPS optimized channel scanning configuration on the access point:

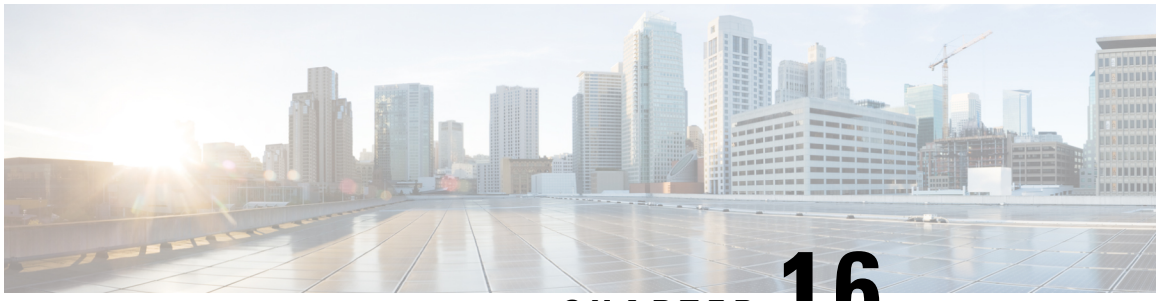
```
Switch# show ap monitor-mode summary
AP Name       Ethernet MAC   Status   Scanning
                                      Channel
                                      List
------------ -------------- -------- ---------
AP1131:4f2.9a 00:16:4:f2:9:a WIPS     1,6,NA,NA
```

This example shows how to display the wIPS configuration forwarded by WCS to the switch:

```
Switch# show wireless wps wips summary
Policy Name.............. Default
Policy Version........... 3
```

This example shows how to display the current state of wIPS operation on the switch:

```
Switch# show wireless wps wips statistics
Policy Assignment Requests..... 1
Policy Assignment Responses..... 1
Policy Update Requests.............. 0
Policy Update Responses............. 0
Policy Delete Requests.............. 0
Policy Delete Responses............. 0
Alarm Updates....................... 13572
Device Updates...................... 8376
Device Update Requests.............. 0
Device Update Responses............. 0
Forensic Updates.................... 1001
Invalid WIPS Payloads............... 0
Invalid Messages Received........... 0
CAPWAP Enqueue Failed............... 0
NMSP Enqueue Failed................. 0
NMSP Transmitted Packets............ 22950
NMSP Transmit Packets Dropped....... 0
NMSP Largest Packet................. 1377
```



CHAPTER 16

Configuring Authentication for Access Points

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Authentication for Access Points

- You can set a global username, password, and enable password for all access points that are currently joined to the switch and any that join in the future inherit as they join the switch. If desired, you can override the global credentials and assign a unique username, password, and enable password for a specific access point.
- After an access point joins the switch, the access point enables console port security, and you are prompted for your username and password whenever you log into the access point's console port. When you log in, you are in nonprivileged mode, and you must enter the enable password in order to use the privileged mode.
- The global credentials that you configure on the switch are retained across switch and access point reboots. They are overwritten only if the access point joins a new switch that is configured with a global username and password. If the new switch is not configured with global credentials, the access point retains the global username and password configured for the first switch.
- You must track the credentials used by the access points. Otherwise, you might not be able to log into an access point's console port. If you need to return the access points to the default *Cisco/Cisco* username

and password, you must clear the switch's configuration and the access point's configuration to return them to factory-default settings. To reset the default access point configuration, enter the **ap name** *Cisco_AP* **mgmtuser username** *Cisco* **password** *Cisco* command. Entering the command does not clear the static IP address of the access point. Once the access point rejoins a switch, it adopts the default *Cisco/Cisco* username and password.

- You can configure global authentication settings for all access points that are currently joined to the switch and any that join in the future. If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point.
- This feature is supported on the following hardware:
  - All Cisco switches that support authentication.
  - Cisco Aironet 1140, 1260, 1310, 1520, 1600, 2600, 3500, and 3600 access points

Restrictions for Configuring Authentication for Access Points

- The switch name in the AP configuration is case sensitive. Therefore, make sure to configure the exact system name on the AP configuration. Failure to do this results in the AP fallback not working.

Information about Configuring Authentication for Access Points

Cisco IOS access points are shipped from the factory with *Cisco* as the default enable password. This password allows users to log into the nonprivileged mode and enter the **show** and **debug** commands that pose a security threat to your network. You must change the default enable password to prevent unauthorized access and to enable users to enter configuration commands from the access point's console port.

You can configure 802.1X authentication between a lightweight access point and a Cisco switch. The access point acts as an 802.1X supplicant and is authenticated by the switch where it uses EAP-FAST with anonymous PAC provisioning.

How to Configure Authentication for Access Points

Configuring Global Credentials for Access Points (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ap mgmtuser username** *user_name* **password 0** *passsword* **secret 0** *secret_value* **Example:** `Switch(config)# ap mgmtuser apusr1 password appass 0 secret 0 appass1`	Configures the global username and password and enables the password for all access points that are currently joined to the switch and any access points that join the switch in the future. In the command, the parameter 0 specifies that an unencrypted password will follow and 8 specifies that an AES encrypted password will follow.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**ap name** *Cisco_AP* **mgmtuser username** *user_name* **password** *password* **secret** *secret* **Example:** `Switch(config)# ap name TSIM_AP-2 mgmtuser apusr1 password appass secret secret`	Overrides the global credentials for a specific access point and assigns a unique username and password and enables password to this access point. The credentials that you enter in this command are retained across switch and access point reboots and if the access point joins a new switch. **Note** If you want to force this access point to use the switch's global credentials, enter the **ap name** *Cisco_AP* **no mgmtuser** command. The following message appears after you execute this command: "AP reverted to global username configuration."
Step 6	**show ap summary** **Example:** `Switch# show ap summary`	Displays a summary of all connected Cisco APs.
Step 7	**show ap name** *Cisco_AP* **config general** **Example:** `Switch# show ap name AP02 config general`	Displays the global credentials configuration for a specific access point. **Note** If this access point is configured for global credentials, the AP User Mode text boxes shows "Automatic." If the global credentials have been overwritten for this access point, the AP User Mode text box shows "Customized."

Configuring Authentication for Access Points (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ap dot1x username** *user_name_value* **password 0** *password_value* **Example:** `Switch(config)# ap dot1x username AP3 password 0 password`	Configures the global authentication username and password for all access points that are currently joined to the switch and any access points that join the switch in the future. This command contains the following keywords and arguments: • **username**—Specifies an 802.1X username for all access points. • *user-id*—Username. • **password**—Specifies an 802.1X password for all access points. • **0**—Specifies an unencrypted password. • **8**—Specifies an AES encrypted password. • *passwd*—Password. **Note** You must enter a strong password for the password parameter. Strong passwords are at least eight characters long, contain a combination of uppercase and lowercase letters, numbers, and symbols, and are not a word in any language.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**ap name** *Cisco_AP* **dot1x-user username** *username_value* **password** *password_value* **Example:**	Overrides the global authentication settings and assigns a unique username and password to a specific access point. This command

	Command or Action	Purpose
	`Switch# ap name AP03 dot1x-user username apuser1 password appass`	contains the following keywords and arguments: • **username**—Specifies to add a username. • *user-id*—Username. • **password**—Specifies to add a password. • **0**—Specifies an unencrypted password. • **8**—Specifies an AES encrypted password. • *passwd*—Password. **Note** You must enter a strong password for the password parameter. See the note in Step 2 for the characteristics of strong passwords. The authentication settings that you enter in this command are retained across switch and access point reboots and whenever the access point joins a new switch.
Step 6	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 7	**no ap dot1x username** *user_name_value* **password 0** *password_value* **Example:** `Switch(config)# no ap dot1x username dot1xusr password 0 dot1xpass`	Disables 802.1X authentication for all access points or for a specific access point. The following message appears after you execute this command: "AP reverted to global username configuration." **Note** You can disable 802.1X authentication for a specific access point only if global 802.1X authentication is not enabled. If global 802.1X authentication is enabled, you can disable 802.1X for all access points only.
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 9	**show ap summary** **Example:**	Displays the authentication settings for all access points that join the switch.

	Command or Action	Purpose
	`Switch# show ap summary`	**Note** If global authentication settings are not configured, the Global AP Dot1x User Name text box shows "Not Configured."
Step 10	**show ap name** *Cisco_AP* **config general** **Example:** `Switch# show ap name AP02 config general`	Displays the authentication settings for a specific access point. **Note** If this access point is configured for global authentication, the AP Dot1x User Mode text boxes shows "Automatic." If the global authentication settings have been overwritten for this access point, the AP Dot1x User Mode text box shows "Customized."

Related Topics

Displaying the Authentication Settings for Access Points: Examples, on page 236

Configuring the Switch for Authentication (CLI)

Note The procedure to perform this task using the switch GUI is not currently available.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**dot1x system-auth-control** **Example:** `Switch(config)# dot1x system-auth-control`	Enables system authentication control.
Step 4	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables new access control commands and functions.

	Command or Action	Purpose
Step 5	**aaa authentication dot1x default group radius** **Example:** `Switch(config)# aaa authentication dot1x default group radius`	Sets the default authentications lists for IEEE 802.1X by using all the radius hosts in a server group.
Step 6	**radius server** *server name* **Example:** `Switch(config)# radius server rsim`	
Step 7	**address** {**ipv4** | **ipv6**} *ip_address* {**auth-port** *port_number* | **acct-port** *port_number*} **Example:** `Switch(config-radius-server)# address ipv4 124.2.2.12 auth-port 1612`	(Optional) Specifies the RADIUS server parameters. For **auth-port port_number**, specify the UDP destination port for authentication requests. The default is 1645. The range is 0 to 65536. For **acct-port port_number**, specify the UDP destination port for authentication requests. The default is 1646.
Step 8	**key** *unencryptied_server_key* **Example:** `Switch(config-radius-server)# key encryptkey`	Sets a clear text encryption key for the RADIUS authentication server.
Step 9	**exit** **Example:** `Switch(config-radius-server)# exit`	Exits the RADIUS server mode and enters the global configuration mode.
Step 10	**interface TenGigabitEthernet1/0/1** **Example:** `Switch(config)# interface TenGigabitEthernet1/0/1`	Sets the 10-Gigbit Ethernet interface. The command prompt changes from Controller(config)# to Controller(config-if)#.
Step 11	**switch mode access** **Example:** `Switch(config-if)# switch mode access`	Sets the unconditional truncking mode access to the interface.
Step 12	**dot1x pae authenticator** **Example:** `Switch(config-if)# dot1x pae authenticator`	Sets the 802.1X interface PAE type as the authenticator.
Step 13	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Displaying the Authentication Settings for Access Points: Examples, on page 236

Configuration Examples for Configuring Authentication for Access Points

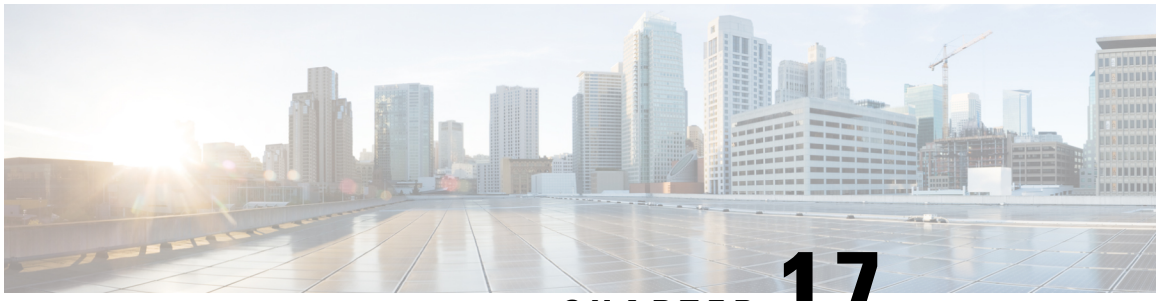
Displaying the Authentication Settings for Access Points: Examples

This example shows how to display the authentication settings for all access points that join the switch:

```
Switch# show ap summary
Number of APs.................................. 1
Global AP User Name............................ globalap
Global AP Dot1x User Name...................... globalDot1x
```

This example shows how to display the authentication settings for a specific access point:

```
Switch# show ap name AP02 config dot11 24ghz general
Cisco AP Identifier............................ 0
Cisco AP Name.................................. TSIM_AP2
...
AP Dot1x User Mode............................. AUTOMATIC
AP Dot1x User Name............................. globalDot1x
```



CHAPTER 17

Converting Autonomous Access Points to Lightweight Mode

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Converting Autonomous Access Points to Lightweight Mode

- Access points that are converted to lightweight mode do not support Wireless Domain Services (WDS). Converted access points communicate only with Cisco wireless LAN switchs and cannot communicate with WDS devices. However, the switch provides functionality that is equivalent to WDS when the access point associates to it.

- All Cisco lightweight access points support 16 Basic Service Set Identifiers (BSSIDs) per radio and a total of 16 wireless LANs per access point. When a converted access point associates to a switch, only wireless LANs with IDs 1 through 16 are pushed to the access point unless the access point is a member of an access point group.
- Access points that are converted to lightweight mode must get an IP address and discover the switch using DHCP, DNS, or IP subnet broadcast.

Information About Autonomous Access Points Converted to Lightweight Mode

You can convert autonomous Cisco Aironet access points to lightweight mode. When you upgrade the access points to lightweight mode, the access point communicates with the switch and receives a configuration and software image from the switch.

Reverting from Lightweight Mode to Autonomous Mode

After you convert an autonomous access point to lightweight mode, you can convert the access point from a lightweight unit back to an autonomous unit by loading a Cisco IOS release that supports autonomous mode (Cisco IOS Release 12.3(7)JA or earlier releases). If the access point is associated with a switch, you can use the switch to load the Cisco IOS release. If the access point is not associated to a switch, you can load the Cisco IOS release using TFTP. In either method, the access point must be able to access a TFTP server that contains the Cisco IOS release to be loaded.

Using DHCP Option 43 and DHCP Option 60

Cisco Aironet Access Points use the type-length-value (TLV) format for DHCP option 43. You must program the DHCP servers to return the option based on the access point's DHCP Vendor Class Identifier (VCI) string (DHCP option 60).

See the product documentation for your DHCP server for instructions on configuring DHCP option 43. The *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode* document contains example steps for configuring option 43 on a DHCP server.

If the access point is ordered with the Service Provider Option - AIR-OPT60-DHCP selected, the VCI string for that access point will be different than those strings listed in the previous table. The VCI string has the following suffix: ServiceProvider. For example, a 1260 with this option returns this VCI string: Cisco AP c1260-ServiceProvider.

Note Ensure that the switch IP address that you obtain from the DHCP server is a unicast IP address. Do not configure the switch IP address as a multicast address when configuring DHCP option 43.

Restrictions for DHCP Option 60

- Cisco Wave2 APs support strings with length up to 256 characters only.

Note When the string length exceeds the limit, the default value is sent during the DHCP discover process.

How Converted Access Points Send Crash Information to the Switch

When a converted access point unexpectedly reboots, the access point stores a crash file on its local flash memory at the time of the crash. After the unit reboots, it sends the reason for the reboot to the switch. If the unit rebooted because of a crash, the switch pulls up the crash file using existing CAPWAP messages and stores it in the switch flash memory. The crash information copy is removed from the access point flash memory when the switch pulls it from the access point.

Uploading Memory Core Dumps from Converted Access Points

By default, access points converted to lightweight mode do not send memory core dumps to the switch. This section provides instructions to upload access point core dumps using the switch GUI or CLI.

Displaying MAC Addresses for Converted Access Points

There are some differences in the way that controllers display the MAC addresses of converted access points on information pages in the controller GUI:

- On the AP Summary page, the controller lists the Ethernet MAC addresses of converted access points.
- On the AP Detail page, the controller lists the BSS MAC addresses and Ethernet MAC addresses of converted access points.
- On the Radio Summary page, the switch lists converted access points by the radio MAC address.

Configuring a Static IP Address for a Lightweight Access Point

If you want to specify an IP address for an access point rather than having one assigned automatically by a DHCP server, you can use the controller GUI or CLI to configure a static IP address for the access point. Static IP addresses are generally used only for deployments with a limited number of APs.

An access point cannot discover the switch using domain name system (DNS) resolution if a static IP address is configured for the access point, unless you specify a DNS server and the domain to which the access point belongs. You can configure these parameters using either the switch CLI or the GUI.

Note If you configure an access point to use a static IP address that is not on the same subnet on which the access point's previous DHCP address was, the access point falls back to a DHCP address after the access point reboots. If the access point falls back to a DHCP address, enter the **show ap config general** *Cisco_AP* CLI command to show that the access point is using a fallback IP address. However, the GUI shows both the static IP address and the DHCP address, but it does not identify the DHCP address as a fallback address.

How to Convert a Lightweight Access Point Back to an Autonomous Access Point

Converting a Lightweight Access Point Back to an Autonomous Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *Cisco_AP* **tftp-downgrade** *tftp_server_ip_address tftp_server_image_filename* **Example:** `Switch# ap name AP02 tftp-downgrade 10.0.0.1 tsrvname`	Converts the lightweight access point back to autonomous mode. **Note** After entering this command, you must wait until the access point reboots and then reconfigure the access point using the CLI or GUI.

Converting a Lightweight Access Point Back to an Autonomous Access Point (Using the Mode Button and a TFTP Server)

Procedure

Step 1 Configure the PC on which your TFTP server software runs with a static IP address in the range of 10.0.0.2 to 10.0.0.30.

Step 2 Make sure that the PC contains the access point image file (such as *c1140-k9w7-tar.123-7.JA.tar* for a 1140 series access point) in the TFTP server folder and that the TFTP server is activated.

Step 3 Rename the access point image file in the TFTP server folder to **c1140-k9w7-tar.default** for a 1140 series access point.

Step 4 Connect the PC to the access point using a Category 5 (CAT5) Ethernet cable.

Step 5 Disconnect power from the access point.

Step 6 Press and hold the **MODE** button while you reconnect power to the access point.

Note The **MODE** button on the access point must be enabled.

Step 7 Hold the **MODE** button until the status LED turns red (approximately 20 to 30 seconds), and release the MODE button.

Step 8 Wait until the access point reboots as indicated by all LEDs turning green followed by the Status LED blinking green.

Step 9 After the access point reboots, reconfigure the access point using the GUI or the CLI.

Authorizing Access Points (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ap auth-list ap-policy authorize-ap** **Example:** `Switch(config)# ap auth-list ap-policy authorize-ap`	Configures an access point authorization policy.
Step 4	**username** *user_name* **mac aaa attribute list** *list_name* **Example:** `Switch(config)# username aaa.bbb.ccc mac aaa attribute list attrlist`	Configures the MAC address of an access point locally.
Step 5	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables new access control commands and functions.
Step 6	**aaa authorization credential-download** *auth_list* **local** **Example:** `Switch(config)# aaa authorization credential-download auth_download local`	Downloads EAP credentials from the local server.
Step 7	**aaa attribute list** *list* **Example:** `Switch(config)# aaa attribute list alist`	Configures AAA attribute list definitions.

	Command or Action	Purpose
Step 8	**aaa session-id common** **Example:** `Switch(config)# aaa session-id common`	Configures the AAA common session ID.
Step 9	**aaa local authentication default authorization default** **Example:** `Switch(config)# aaa local authentication default authorization default`	Configures the local authentication method list.
Step 10	**show ap name** *Cisco_AP* **config general** **Example:** `Switch(config)# show ap name AP01 config general`	Displays the configuration information that corresponds to a specific access point.

Authorizing Access Points (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **AP Policy**.

The **AP Policy** page is displayed.

Step 2 In the Policy Configuration area, enable or disable the following parameters:

- **Authorize LSC APs against Auth-List**
- **AP with Self-Signed Certificate**
- **Authorize MIC APs against AAA**
- **AP with Manufacturing Installed Certificate**

Step 3 Click **Apply**.

Step 4 Click **Save Configuration**.

Disabling the Reset Button on Converted Access Points (CLI)

You can enable or disable the Reset button on access points that are converted to lightweight mode. The Reset button is labeled MODE on the outside of the access point.

Note The procedure to perform this task using the controller GUI is not currently available.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**no ap reset-button** **Example:** `Switch(config)# no ap reset-button`	Disables the Reset buttons on all converted access points that are associated to the switch. **Note** To enable the Reset buttons on all converted access points that are associated to the switch, enter the **ap reset-button** command.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**ap name** *Cisco_AP* **reset-button** **Example:** `Switch# ap name AP02 reset-button`	Enables the Reset button on the converted access point that you specify.

Monitoring the AP Crash Log Information

Note The procedure to perform this task using the switch GUI is not currently available.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**show ap crash-file** **Example:** `Switch# show ap crash-file`	Verifies whether the crash file is downloaded to the switch.

How to Configure a Static IP Address on an Access Point

Configuring a Static IP Address on an Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *Cisco_AP* **static-ip ip-address** *static_ap_address* **netmask** *static_ip_netmask* **gateway** *static_ip_gateway* **Example:** `Switch# ap name AP03 static-ip ip-address 9.9.9.16 netmask 255.255.0.0 gateway 9.9.9.2`	Configures a static IP address on the access point. This command contains the following keywords and arguments: • **ip-address**— Specifies the Cisco access point static IP address. • *ip-address*— Cisco access point static IP address. • **netmask**—Specifies the Cisco access point static IP netmask. • *netmask*— Cisco access point static IP netmask. • **gateway**—Specifies the Cisco access point gateway. • *gateway*— IP address of the Cisco access point gateway. The access point reboots and rejoins the switch, and the static IP address that you specify is pushed to the access point. After the static IP address has been sent to the access point, you can configure the DNS server IP address and domain name. You must perform Steps 3 and 4 after the access points reboot.
Step 3	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 4	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 5	**ap static-ip name-server** *nameserver_ip_address* **Example:** `Switch(config)# ap static-ip name-server 10.10.10.205`	Configures a DNS server so that a specific access point or all access points can discover the switch using DNS resolution. **Note** To undo the DNS server configuration, enter the **no ap static-ip name-server** *nameserver_ip_address* command.
Step 6	**ap static-ip domain** *static_ip_domain* **Example:** `Switch(config)# ap static-ip domain domain1`	Configures the domain to which a specific access point or all access points belong. **Note** To undo the domain name configuration, enter the **no ap static-ip domain** *static_ip_domain* command.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 8	**show ap name** *Cisco_AP* **config general** **Example:** `Switch# show ap name AP03 config general`	Displays the IP address configuration for the access point.

Configuring a Static IP Address on an Access Point (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points** > **All APs**.

The **All APs** page is displayed.

Step 2 Click the name of the access point.

The **AP > Edit** page is displayed.

Step 3 In the **General** tab, in the **IP Config** area, select the **Static IP** check box if you want to assign a static IP address to the access point.

Step 4 Enter the following details:

- **Static IP**
- **Netmask**
- **Gateway**

Step 5 Click **Apply**.

The access point reboots and rejoins the switch, and the static IP address that you specified is sent to the access point.

Step 6 After the static IP address has been sent to the access point, configure the **DNS IP Address** and **Domain Name**.

Step 7 Click **Apply**.

Step 8 Click **Save Configuration**.

Recovering the Access Point Using the TFTP Recovery Procedure

Procedure

Step 1 Download the required recovery image from Cisco.com (ap3g2-k9w8-tar.152-2.JA.tar) and install it in the root directory of your TFTP server.

Step 2 Connect the TFTP server to the same subnet as the target access point and power-cycle the access point. The access point boots from the TFTP image and then joins the switch to download the oversized access point image and complete the upgrade procedure.

Step 3 After the access point has been recovered, you can remove the TFTP server.

Configuration Examples for Converting Autonomous Access Points to Lightweight Mode

Displaying the IP Address Configuration for Access Points: Example

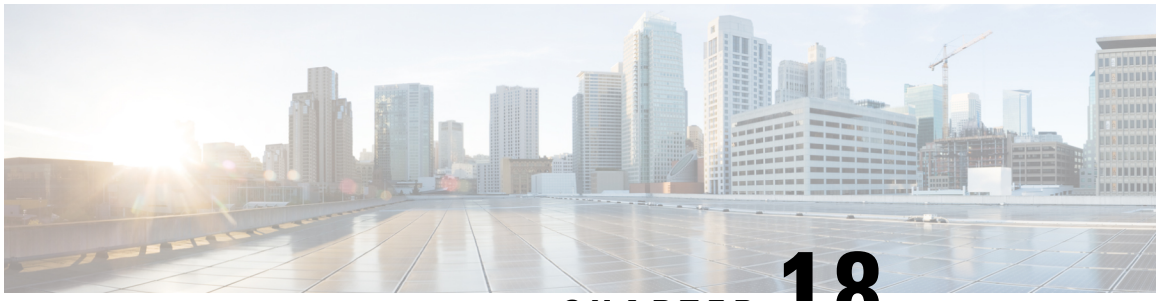
This example shows how to display the IP address configuration for the access point:

```
Switch# show ap name AP03 dot11 24ghz config general
Cisco AP Identifier.............. 4
Cisco AP Name.................................... AP6
IP Address Configuration..................... Static IP assigned
IP Address....................................... 10.10.10.118
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 10.10.10.1
Domain........................................... Domain1
Name Server...................................... 10.10.10.205
...
```

Displaying Access Point Crash File Information: Example

This example shows how to display access point crash file information. Using this command, you can verify whether the file is downloaded to the switch:

```
Switch# show ap crash-file
Local Core Files:
lrad_AP1130.rdump0 (156)

The number in parentheses indicates the size of the file. The size should
be greater than zero if a core dump file is available.
```



CHAPTER 18

Using Cisco Workgroup Bridges

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Cisco Workgroup Bridges and non-Cisco Workgroup bridges

A WGB is a mode that can be configured on an autonomous Cisco IOS access point to provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the WGB access point. A WGB connects a wired network over a single wireless segment by learning the MAC addresses of its wired clients on the Ethernet interface and reporting them to the lightweight access point using Internet Access Point Protocol (IAPP) messaging. The WGB provides wireless access connectivity to wired clients by establishing a single wireless connection to the lightweight access point.

When a Cisco WGB is used, the WGB informs the access points of all the clients that it is associated with. The switch is aware of the clients that are associated with the access point. When non-Cisco WGBs are used, the switch has no information about the IP address of the clients on the wired segment behind the WGB. Without this information, the switch drops the following types of messages:

- ARP REQ from the distribution system for the WGB client.
- ARP RPLY from the WGB client.
- DHCP REQ from the WGB client.

• DHCP RPLY for the WGB client.

Monitoring the Status of Workgroup Bridges

Note The procedure to perform this task using the switch GUI is not currently available.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**show wireless wgb summary** **Example:** `Switch# show wireless wgb summary`	Displays the WGBs on your network.
Step 3	**show wireless wgb mac-address** *wgb_mac_address* **detail** **Example:** `Switch# show wireless wgb mac-address 00:0d:ed:dd:25:82 detail`	Displays the details of any wired clients that are connected to a particular WGB.

Debugging WGB Issues (CLI)

Note The procedure to perform this task using the switch GUI is not currently available.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**debug iapp all** **Example:** `Switch# debug iapp all`	Enables debugging for IAPP messages.

	Command or Action	Purpose
Step 3	**debug iapp error** **Example:** `Switch# debug iapp error`	Enables debugging for IAPP error events.
Step 4	**debug iapp packet** **Example:** `Switch# debug iapp packet`	Enables debugging for IAPP packets.
Step 5	**debug mobility handoff** [**switch** *switch_number*] **Example:** `Switch# debug mobility handoff`	Enables debugging for any roaming issues.
Step 6	**debug dhcp** **Example:** `Switch# debug dhcp`	Debug an IP assignment issue when DHCP is used.
Step 7	**debug dot11 mobile** **Example:** `Switch# debug dot11 mobile`	Enables dot11/mobile debugging. Debug an IP assignment issue when static IP is used.
Step 8	**debug dot11 state** **Example:** `Switch# debug dot11 state`	Enables dot11/state debugging. Debug an IP assignment issue when static IP is used.

Configuration Examples for Configuring Workgroup Bridges

WGB Configuration: Example

This example shows how to configure a WGB access point using static WEP with a 40-bit WEP key:

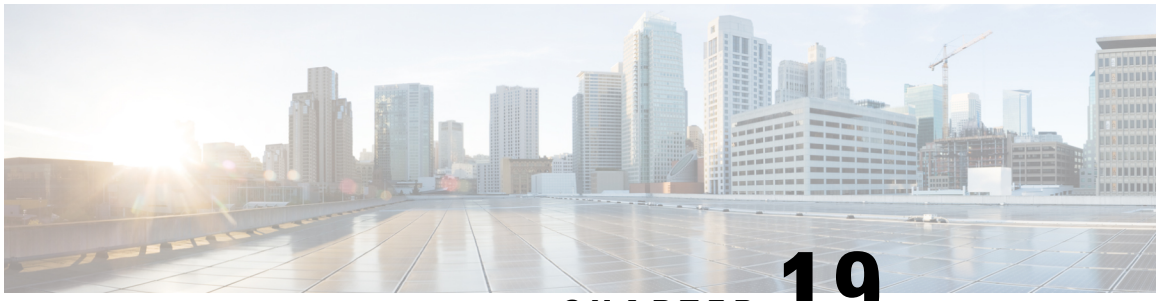
```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# dot11 ssid WGB_with_static_WEP
Switch(config-ssid)# authentication open
Switch(config-ssid)# guest-mode
Switch(config-ssid)# exit
Switch(config)# interface  dot11Radio 0
Switch(config)# station-role workgroup-bridge
Switch(config-if)# encry mode wep 40
Switch(config-if)# encry key 1 size 40 0 1234567890
Switch(config-if)# ssid WGB_with_static_WEP
Switch(config-if)# end
```

Verify that the WGB is associated to an access point by entering this command on the WGB:

show dot11 association

Information similar to the following appears:

```
Switch# show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [FCVTESTING] :
MAC Address    IP address      Device        Name            Parent         State
000b.8581.6aee 10.11.12.1      WGB-client    map1            -              Assoc
ap#
```



CHAPTER 19

Configuring Probe Request Forwarding

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configuring Probe Request Forwarding

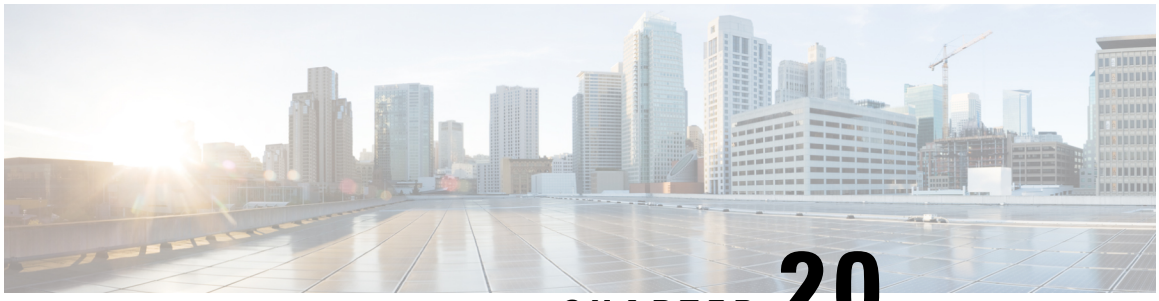
Probe requests are 802.11 management frames that are sent by clients to request information about the capabilities of Service Set Identifiers (SSIDs). By default, access points forward acknowledged probe requests to the switch for processing. Acknowledged probe requests are probe requests for SSIDs that are supported by the access point. If desired, you can configure access points to forward both acknowledged and unacknowledged probe requests to the switch. The switch can use the information from unacknowledged probe requests to improve the location accuracy.

How to Configure Probe Request Forwarding (CLI)

Note The procedure to perform this task using the switch GUI is not currently available.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wireless probe filter** **Example:** `Switch(config)# wireless probe filter`	Enables or disables the filtering of probe requests forwarded from an access point to the switch. **Note** If you enable probe filtering, the default filter setting, the access point forwards only acknowledged probe requests to the switch. If you disable probe filtering, the access point forwards both acknowledged and unacknowledged probe requests to the switch.
Step 3	**wireless probe limit** *num_probes interval* **Example:** `Switch(config)# wireless probe limit 10 1000`	Limits the number of probe requests sent to the switch per client per access point radio in a given interval. You must specify the following arguments with this command: • *num_probes*—Number of probe requests forwarded to the switch per client per access point radio in a given interval. The range is from 1 to 100. • *interval*—Probe limit interval in milliseconds. The range is from 100 to 10000.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**show wireless probe** **Example:** `Switch# show wireless probe`	Displays the advanced probe request configuration.



CHAPTER 20

Optimizing RFID Tracking

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Optimizing RFID Tracking on Access Points

To optimize the monitoring and location calculation of RFID tags, you can enable tracking optimization on up to four channels within the 2.4-GHz band of an 802.11b/g access point radio. This feature allows you to scan only the channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

How to Optimize RFID Tracking on Access Points

Optimizing RFID Tracking on Access Points (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap name** *Cisco_AP* **mode monitor submode none** **Example:**	Specifies the monitor submode for the access point as none.

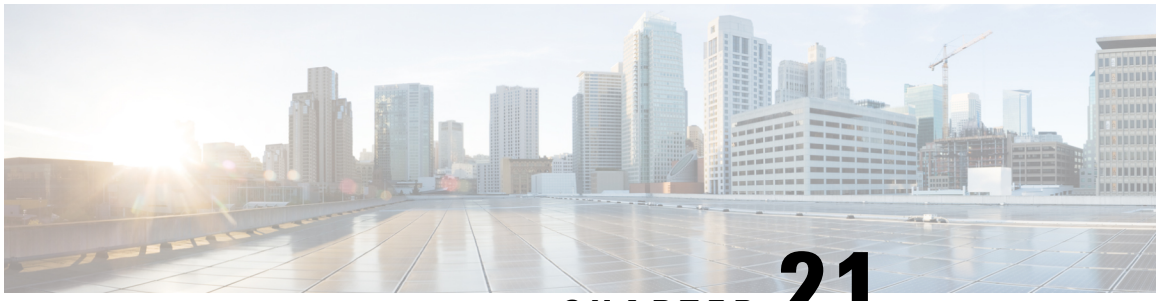
	Command or Action	Purpose
	`Switch# ap name 3602a mode monitor submode none`	**Note** A warning message indicates that changing the access point's mode will cause the access point to reboot and prompts you to specify whether you want to continue by entering **Y**. After you enter **Y**, the access point reboots.
Step 2	**ap name** *Cisco_AP* **dot11 24ghz shutdown** **Example:** `Switch# ap name AP01 dot11 24ghz shutdown`	Disables the access point radio.
Step 3	**ap name** *Cisco_AP* **monitor-mode tracking-opt** **Example:** `Switch# ap name TSIM_AP1 monitor-mode tracking-opt`	Configures the access point to scan only the Dynamic Channel Assignment (DCA) channels supported by its country of operation. **Note** To disable tracking optimization for an access point, enter the **ap name** *Cisco_AP* **monitor-mode tracking-opt no-optimization** command.
Step 4	**ap name** *Cisco_AP* **monitor-mode dot11b** {**fast-channel** [*first_channel second_channel third_channel fourth_channel*]} **Example:** `Switch# ap name AP01 monitor-mode dot11b fast-channel 1 2 3 4`	Chooses up to four specific 802.11b channels to be scanned by the access point. **Note** In the United States, you can assign any value from 1 to 11 (inclusive) to the channel variable. Other countries support additional channels. You must assign at least one channel.
Step 5	**ap name** *Cisco_AP* **no dot11 24ghz shutdown** **Example:** `Switch# ap name AP01 no dot11 24ghz shutdown`	Enables the access point radio.
Step 6	**show ap monitor-mode summary** **Example:** `Switch# show ap monitor-mode summary`	Displays all the access points in monitor mode.

Configuration Examples for Optimizing RFID Tracking

Displaying all the Access Points in Monitor Mode: Example

This example shows how to display all the access points in monitor mode:

```
Switch# show ap monitor-mode summary

AP Name       Ethernet MAC   Status   Scanning
                                      Channel
                                      List
------------- -------------- -------- ---------
AP1131:4f2.9a 00:16:4:f2:9:a Tracking 1,6,NA,NA
```



CHAPTER 21

Configuring Country Codes

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Country Codes

Controllers and access points are designed for use in many countries with varying regulatory requirements. The radios within the access points are assigned to a specific regulatory domain at the factory (such as -E for Europe), but the country code enables you to specify a particular country of operation (such as FR for France or ES for Spain). Configuring a country code ensures that each radio's broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations.

Information About Japanese Country Codes

Country codes define the channels that can be used legally in each country. These country codes are available for Japan:

- JP—Allows only -J radios to join the controller
- J2—Allows only -P radios to join the controller
- J3—Uses the -U frequencies, but allows -U, -P, and -Q (other than 1550/1600/2600/3600) radios to join the WLC
- J4—Allows 2.4G JPQU and 5G PQU to join the controller.

Note The 1550, 1600, 2600, and 3600 APs require J4.

See the Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points document for the list of channels and power levels supported by access points in the Japanese regulatory domains.

Prerequisites for Configuring Country Codes

- Generally, you should configure one country code per switch; you configure one code that matches the physical location of the switch and its access points. You can configure up to 20 country codes per switch. This multiple-country support enables you to manage access points in various countries from a single switch.
- When the multiple-country feature is used, all the switchs that are going to join the same RF group must be configured with the same set of countries, configured in the same order.
- Access points are capable of using all the available legal frequencies. However, access points are assigned to the frequencies that are supported in their relevant domains.
- The country list configured on the RF group leader determines which channels the members will operate on. This list is independent of which countries have been configured on the RF group members.
- For switchs in the Japan regulatory domain, you should have one or more Japan country codes (JP, J2, or J3) configured on your switch at the time you last booted your switch.
- For switchs in the Japan regulatory domain, you must have at least one access point with a -J regulatory domain joined to your switch.

How to Configure Country Codes

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**show wireless country supported** **Example:** `Switch# show wireless country supported`	Displays a list of all the available country codes.
Step 3	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 4	**ap dot11 24ghz shutdown** **Example:** `Switch(config)# ap dot11 5ghz shutdown`	Disables the 802.11b/g network.
Step 5	**ap dot11 5ghz shutdown** **Example:** `Switch(config)# ap dot11 24ghz shutdown`	Disables the 802.11a network.
Step 6	**ap country** *country_code* **Example:** `Switch(config)# ap country IN`	Assigns access points to a specific country. **Note** Make sure that the country code you choose is compatible with the regulatory domain of at least one of the access point's radios.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 8	**show wireless country channels** **Example:** `Switch# show wireless country channels`	Displays the list of available channels for the country codes configured on your switch. **Note** Perform Steps 9 through 17 only if you have configured multiple country codes in Step 6.
Step 9	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 10	**no ap dot11 5ghz shutdown** **Example:** `Switch(config)# no ap dot11 5ghz shutdown`	Enables the 802.11a network.
Step 11	**no ap dot11 24ghz shutdown** **Example:** `Switch(config)# no ap dot11 24ghz shutdown`	Enables the 802.11b/g network.
Step 12	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 13	**ap name** *cisco-ap* **shutdown** **Example:**	Disables the access point.

	Command or Action	Purpose
	`Switch# ap name AP02 shutdown`	**Note** Ensure that you disable only the access point for which you are configuring country codes.
Step 14	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 15	**ap country** *country_code* **Example:** `Switch# ap country IN`	Assigns an access point to a specific country. **Note** • If you enabled the networks and disabled some access points and then enter the **ap country** *country_code* command, the specified country code is configured on only the disabled access points. All other access points are ignored. • Ensure that the country code that you choose is compatible with the regulatory domain of at least one of the access point's radios.
Step 16	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 17	**ap name** *cisco-ap* **no shutdown** **Example:** `Switch# ap name AP02 no shutdown`	Enables the access point.

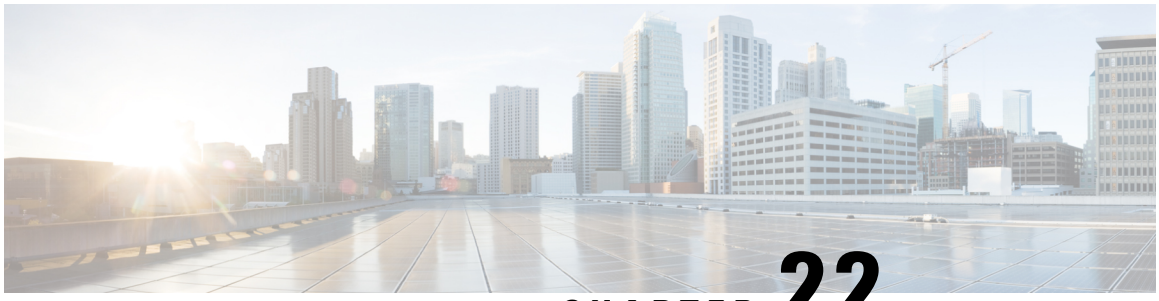
Configuration Examples for Configuring Country Codes

Displaying Channel List for Country Codes: Example

This example shows how to display the list of available channels for the country codes configured on your switch:

```
Switch# show wireless country channels

Configured Country.....................: US - United States
KEY: * = Channel is legal in this country and may be configured manually.
     A = Channel is the Auto-RF default in this country.
```

```
     . = Channel is not legal in this country.
     C = Channel has been configured for use by Auto-RF.
     x = Channel is available to be configured for use by Auto-RF.
  (-,-) = (indoor, outdoor) regulatory domain allowed by this country.
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11bg         :
Channels         :                  1 1 1 1 1
                  1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
(-A ,-AB ) US    : A * * * * A * * * * A . . .
Auto-RF          : . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11a          :                        1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels         :3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
                  4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
(-A ,-AB ) US    : . A . A . A . A A A A A * * * * * . . . * * * A A A A*
Auto-RF          : . . . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
4.9GHz 802.11a   :
Channels         :                  1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
                  1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
US (-A ,-AB )    : * * * * * * * * * * * * * * * * * * * A * * * * * A
Auto-RF          : . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```



CHAPTER 22

Configuring Link Latency

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Link Latency

- The switch displays the current round-trip time as well as a running minimum and maximum round-trip time. The minimum and maximum times continue to run as long as the switch is up or can be cleared and allowed to restart.
- You can configure link latency for a specific access point using the switch GUI or CLI or for all access points joined to the switch using the CLI.

Restrictions for Configuring Link Latency

- Link latency calculates the Control and Provisioning of Wireless Access Points (CAPWAP) response time between the access point and the switch. It does not measure network latency or ping responses.

Information About Configuring Link Latency

You can configure link latency on the switch to measure the link between an access point and the switch. You can use this feature with all access points that are joined to the switch where the link can be a slow or unreliable WAN connection.

TCP MSS

If the client's maximum segment size (MSS) in a Transmission Control Protocol (TCP) three-way handshake is greater than the maximum transmission unit can handle, the client might experience reduced throughput and the fragmentation of packets. To avoid this problem, you can specify the MSS for all access points that are joined to the switch or for a specific access point.

When you enable this feature, the access point selects the MSS for TCP packets to and from wireless clients in its data path. If the MSS of these packets is greater than the value that you configured or greater than the default value for the CAPWAP tunnel, the access point changes the MSS to the new configured value.

Link Tests

A link test is used to determine the quality of the radio link between two devices. Two types of link-test packets are transmitted during a link test: request and response. Any radio receiving a link-test request packet fills in the appropriate text boxes and echoes the packet back to the sender with the response type set.

The radio link quality in the client-to-access point direction can differ from that in the access point-to-client direction due to the asymmetrical distribution of the transmit power and receive sensitivity on both sides. Two types of link tests can be performed: a ping test and a CCX link test.

With the *ping link test*, the controller can test link quality only in the client-to-access point direction. The RF parameters of the ping reply packets received by the access point are polled by the controller to determine the client-to-access point link quality.

With the *CCX link test*, the switch can also test the link quality in the access point-to-client direction. The switch issues link-test requests to the client, and the client records the RF parameters (received signal strength indicator [RSSI], signal-to-noise ratio [SNR], and so on) of the received request packet in the response packet. Both the link-test requestor and responder roles are implemented on the access point and switch. Not only can the access point or switch initiate a link test to a CCX v4 or v5 client, but a CCX v4 or v5 client can initiate a link test to the access point or switch.

The switch shows the link-quality metrics for CCX link tests in both directions (out— the access point to the client; in— the client to the access point):

- Signal strength in the form of RSSI (minimum, maximum, and average)
- Signal quality in the form of SNR (minimum, maximum, and average)
- Total number of packets that are retried
- Maximum retry count for a single packet
- Number of lost packets
- Data rate of a successfully transmitted packet

The controller shows this metric regardless of direction:

- Link test request/reply round-trip time (minimum, maximum, and average)

The controller software supports CCX versions 1 through 5. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. The controller stores the CCX version of the client in its client database and uses it to limit the features for this client. If a client does not support CCXv4 or v5, the controller performs a ping link test on the client. If a client supports CCXv4 or v5, the controller performs a CCX link test on the client. If a client times out during a CCX link test, the controller switches to the ping link test automatically.

How to Configure Link Latency

Configuring Link Latency (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ap link-latency** **Example:** `Switch(config)# ap link-latency`	Enables link latency for all access points that are currently associated with the switch. **Note** To disable link latency for all the access points that are associated with the switch, use the **no ap link-latency** command. **Note** These commands enable or disable link latency only for access points that are currently joined to the switch. You have to enable or disable link latency for the access points that join in the future.

	Command or Action	Purpose
		Note To enable or disable link latency for specific access points that are associated with the switch, enter the following commands in Priveleged EXEC mode: • **ap name** *Cisco_AP* **link-latency**—Enables link latency. • **ap name** *Cisco_AP* **no link-latency**—Disables link latency.
Step 4	**ap tcp-adjust-mss size** *size* **Example:** `Switch(config)# ap tcp-adjust-mss size 537`	Configures TCP MSS adjust size for all access points. The range is from 536 to 1363.
Step 5	**show ap name** *Cisco_AP* **config general** **Example:** `Switch(config)# show ap name AP02 config general`	Displays the general configuration details of the access point. These configuration details contain the link latency results that correspond to the access point that you specify in the command. The output of this command contains the following link latency results: • Current Delay—The current round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the switch and back. • Maximum Delay—Since the time that link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the switch and back. • Minimum Delay—Since the time that link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the switch and back.
Step 6	**ap name** *Cisco_AP* **link-latency** [**reset**] **Example:** `Switch(config)# ap name AP02 link-latency reset`	Clears the current, minimum, and maximum link latency statistics on the switch for a specific access point.

	Command or Action	Purpose
Step 7	**show ap name** *Cisco_AP* **config general** **Example:** `Switch(config)# show ap name AP02 config general`	Displays the general configuration details of the access point. Use this command to see the result of the reset operation.

Configuring Link Latency (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points** > **All APs**.

The **All APs** page appears with a list of access points.

Step 2 Click the name of the access point.

The **AP > Edit** page appears.

Step 3 Click the **Advanced** tab.

Step 4 In the **Link Latency** area, select or unselect the **Enable Link Latency** check box.

Note You can select the **Enable Link Latency** check box to enable link latency for this access point or unselect it to prevent the access point from sending the round-trip time to the switch after every echo response is received. The default state is unselected.

Step 5 Click **Apply**.

Step 6 When a message box appears that indicates that AP Parameters are modified successfully, click **OK**.

Step 7 When the **All APs** page is displayed, click the access point that you have modified earlier.

The **AP > Edit** page appears.

Step 8 Click the **Advanced** tab.

In the **Link Latency** area, the following link latency and data latency results are displayed:

- **Current(mSec)**—The current round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the switch and back.
- **Minimum(mSec)**—Since the time that link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the switch and back.
- **Maximum(mSec)**—Since the time that link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the switch and back.

Step 9 Click **Reset Link Latency** to clear the current, minimum, and maximum link latency and data latency statistics on the switch for this access point.

Note After the page refreshes and the **All APs** page is displayed again, click the **Advanced** tab. The updated statistics appear in the **Minimum** and **Maximum** text boxes.

How to Configure TCP MSS

Configuring TCP MSS (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap tcp-adjust-mss size** *size_value* **Example:** `Switch(config)# ap tcp-adjust-mss size 537`	Enables the TCP MSS on the particular access point that you specify. **Note** To enable TCP MSS on all the access points that are associated with the switch, enter the **ap tcp-adjust-mss size** *size_value* command, where the size parameter is from 536 to 1363 bytes. The default value varies for different clients.
Step 3	**reload** **Example:** `Switch# reload`	Reboots the switch in order for your change to take effect.
Step 4	**show ap tcp-adjust-mss** **Example:** `Switch# show ap tcp-adjust-mss`	Displays the current TCP MSS setting for all the access points that are associated with the switch. **Note** To display the TCP MSS settings that correspond to a specific access point, enter the **show ap name** *Cisco_AP* **tcp-adjust-mss** command.

Configuring TCP MSS (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points** > **Global AP Configuration**.

The **Global Configuration** page is displayed.

Step 2 In the **TCP MSS** area, select the **Global TCP Adjust MSS** check box and set the MSS for all access points that are associated with the switch. The valid range is from 536 to 1363 bytes.

Step 3 Click **Apply**.

Step 4 Click **Save Configuration**.

Performing a Link Test (CLI)

Note The procedure to perform this task using the switch GUI is not currently available.

Procedure

	Command or Action	Purpose
Step 1	**test wireless linktest** *mac_address* **Example:** `Switch# test wireless linktest 00:0d:88:c5:8a:d1`	Runs a link test.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**wireless linktest frame-size** *frame_size* **Example:** `Switch(config)# wireless linktest frame-size 41`	Configures the link test frame size for each packet.
Step 4	**wireless linktest number-of-frames** *number_of_frames* **Example:** `Switch(config)# wireless linktest number-of-frames 50`	Configures the number of frames to send for the link test.

	Command or Action	Purpose
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuration Examples for Configuring Link Latency

Running a Link Test: Example

This example shows how to run a link test:

```
Switch# test wireless linktest 6470.0227.ca55
Switch# show wireless linktest statistic

Link Test to 64700227CA55 with 500 frame-size.
Client MAC Address                          : 6470.0227.ca55
AP Mac Address                              : 44e4.d901.19c0
Link Test Packets Sent                      : 20
Link Test Packets Received                  : 20
Link Test Pkts Lost(Total/AP->Clnt/Clnt->AP) : 0/0/0
Link Test Pkts round trip time (min/max/avg) : 9ms/31ms/14ms
RSSI at AP (min/max/average)                : -53dBm/-51dBm/-52dBm
RSSI at Client (min/max/average)            : -48dBm/-40dBm/-44dBm
```

Displaying Link Latency Information: Example

This example shows how to display general configuration details of the access point. These configuration details contain the link latency results that correspond to the access point that you specify in the command.

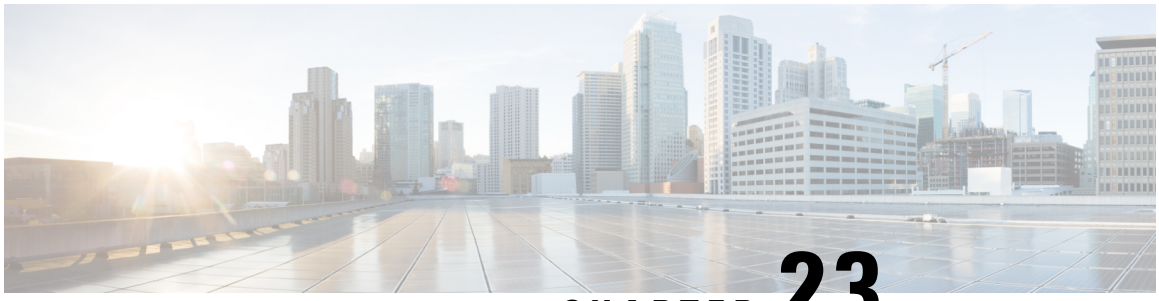
```
Switch# show ap name AP01 config general

Cisco AP Name                                   : AP01
Cisco AP Identifier                             : 55
Country Code                                    : US  - United States
Regulatory Domain Allowed by Country            : 802.11bg:-A     802.11a:-A
AP Country Code                                 : US  - United States
AP Regulatory Domain                            : Unconfigured
Switch Port Number                              : Te1/0/1
MAC Address                                     : 0000.2000.03f0
IP Address Configuration                        : Static IP assigned
IP Address                                      : 9.9.9.16
IP Netmask                                      : 255.255.0.0
Gateway IP Address                              : 9.9.9.2
Fallback IP Address Being Used                  : 9.9.9.16
Domain                                          : Cisco
Name Server                                     : 0.0.0.0
CAPWAP Path MTU                                 : 1485
Telnet State                                    : Enabled
SSH State                                       : Disabled
Cisco AP Location                               : default-location
Cisco AP Group Name                             : default-group
Primary Cisco Controller Name                   : CAPWAP Controller
Primary Cisco Controller IP Address             : 9.9.9.2
Secondary Cisco Controller Name                 :
```

```
Secondary Cisco Controller IP Address           : Not Configured
Tertiary Cisco Controller Name                  :
Tertiary Cisco Controller IP Address            : Not Configured
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : Local
AP Submode                                      : Not Configured
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : informational
Software Version                                : 7.4.0.5
Boot Version                                    : 7.4.0.5
Stats Reporting Period                          : 180
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : Power Injector/Normal Mode
Number of Slots                                 : 2
AP Model                                        : 3502E
AP Image                                        : C3500-K9W8-M
IOS Version                                     :
Reset Button                                    :
AP Serial Number                                : SIM1140K002
AP Certificate Type                             : Manufacture Installed
Management Frame Protection Validation          : Disabled
AP User Mode                                    : Customized
AP User Name                                    : Not Configured
AP 802.1X User Mode                             : Not Configured
AP 802.1X User Name                             : Not Configured
Cisco AP System Logging Host                    : 255.255.255.255
AP Up Time                                      : 16 days 3 hours 14 minutes 1 s
econd
AP CAPWAP Up Time                               : 33 minutes 15 seconds
Join Date and Time                              : 01/02/2013 22:41:47
Join Taken Time                                 : 16 days 2 hours 40 minutes 45
seconds
Join Priority                                   : 1
Ethernet Port Duplex                            : Auto
Ethernet Port Speed                             : Auto
AP Link Latency                                 : Enabled
Current Delay                                   : 0
Maximum Delay                                   : 0
Minimum Delay                                   : 0
Last Updated (based on AP up time)              : 0 seconds
Rogue Detection                                 : Disabled
AP TCP MSS Adjust                               : Disabled
AP TCP MSS Size                                 : 536
```

Displaying TCP MSS Settings: Example

This example shows how to display the current TCP MSS setting for all the access points that are associated with the switch:

```
Switch# show ap tcp-adjust-mss

AP Name                    TCP State        MSS Size
-----------------------------------------------------
AP01                       Disabled         6146
AP02                       Disabled         536
AP03                       Disabled         6146
AP04                       Disabled         6146
AP05                       Disabled         6146
```



CHAPTER 23

Configuring Power over Ethernet

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configuring Power over Ethernet

When an access point that has been converted to lightweight mode (such as an AP1262) access point is powered by a power injector that is connected to a Cisco pre-Intelligent Power Management (pre-IPM) switch, you must configure Power over Ethernet (PoE), which is also known as *inline power*.

How to Configure Power over Ethernet

Configuring Power over Ethernet (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap name** *Cisco_AP* **power injector installed** **Example:**	Enables the PoE power injector state. The access point remembers that a power injector is connected to this particular switch port. If you relocate the access point, you must reenter

	Command or Action	Purpose
	`Switch# ap name AP02 power injector installed`	this command after the presence of a new power injector is verified. **Note** Enter this command if your network contains any older Cisco 6-W switches that could be accidentally overloaded if connected directly to a 12-W access point. Make sure that the Cisco Discovery Protocol (CDP) is enabled before entering this command. Otherwise, this command will fail.
Step 2	**ap name** *Cisco_AP* **power injector override** **Example:** `Switch# ap name AP02 power injector override`	Removes the safety checks and allows the access point to be connected to any switch port. You can use this command if your network does not contain any older Cisco 6-W switches that could be overloaded if connected directly to a 12-W access point. The access point assumes that a power injector is always connected. If you relocate the access point, it continues to assume that a power injector is present.
Step 3	**ap name** *Cisco_AP* **power injector switch-mac-address** *switch_mac_address* **Example:** `Switch# ap name AP02 power injector switch-mac-address 10a.2d.5c.3d`	Sets the MAC address of the switch port that has a power injector. **Note** Enter this command if you know the MAC address of the connected switch port and do not want to automatically detect it using the installed option.
Step 4	**show ap name** *Cisco_AP* **config general** **Example:** `Switch# show ap name AP02 config general`	Displays common information that includes the PoE settings for a specific access point. **Note** The Power Type/Mode text box shows "degraded mode" if the access point is not operating at full power.

Configuring Power over Ethernet (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points** > **All APs**.

The **All APs** page appears with a list of access points that are associated with the switch.

Step 2 Click the name of the access point.

The **AP > Edit** page appears.

Step 3 Click the **Advanced** tab.

Step 4 In the **Power Over Ethernet Settings** area, select the **Pre-Standard 802.3af Switches** check box.

Select this check box if the access point is being powered by a high-power 802.3af Cisco switch. This switch provides more than the traditional 6 Watts of power but does not support the intelligent power management (IPM) feature.

Note Unselect the **Pre-standard 802.3af Switches** check box if power is being provided by a power injector. This is the default value.

Step 5 Select the **Power Injector State** check box.

Select this check box if the attached switch does not support IPM and a power injector is being used. If the attached switch supports IPM, you do not need to select this check box.

The **Power Injector Selection** drop-down list is displayed that contains parameters that enable you to protect your switch port from an accidental overload if the power injector is inadvertently bypassed.

Step 6 From the **Power Injector Selection** drop-down list, choose an option to specify the desired level of protection.

You can choose any one of the following three options:

- **Installed**—Examines and remembers the MAC address of the currently connected switch port and assumes that a power injector is connected. Choose this option if your network contains older Cisco 6-Watt switches and you want to avoid possible overloads by forcing a double-check of any relocated access points.

  If you want to configure the switch MAC address, enter the MAC address in the **Injector Switch MAC Address** text box. If you want the access point to find the switch MAC address, leave the **Injector Switch MAC Address** text box blank.

  Note Each time that an access point is relocated, the MAC address of the new switch port fails to match the remembered MAC address, and the access point remains in low-power mode. You must then physically verify the existence of a power injector and reselect this option to cause the new MAC address to be remembered.

- **Override**—Allows the access point to operate in high-power mode without first verifying a matching MAC address. You can use this option if your network does not contain any older Cisco 6-W switches that could be overloaded if connected directly to a 12-W access point. The advantage of this option is that if you relocate the access point, it continues to operate in high-power mode without any further configuration. The disadvantage of this option is that if the access point is connected directly to a 6-W switch, an overload occurs.

Step 7 Click **Apply**.

Step 8 Click **Save Configuration**.

What to do next

Manually reset the access point in order for the change to take effect.

Configuration Examples for Configuring Power over Ethernet

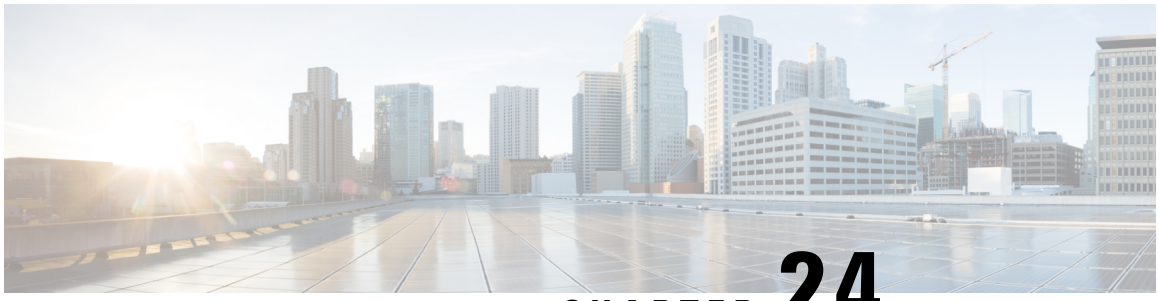
Displaying Power over Ethernet Information: Example

This example shows how to display common information that includes the PoE settings for a specific access point:

```
Switch# show ap name AP01 config general

Cisco AP Identifier.............. 1
Cisco AP Name.................... AP1
...
PoE Pre-Standard Switch.......... Enabled
PoE Power Injector MAC Addr...... Disabled
Power Type/Mode.................. PoE/Low Power (degraded mode)
...
```

PART VI

Mobility



CHAPTER 24

Information About Mobility

Overview

The switch delivers more services at access layer other than merely providing increased speeds and feeds. Wireless services is now integrated with the switch, which ensures that the access layer switch terminates the wireless users data plane, thereby delivering on the promise of Cisco's unified architecture. Unification implies that mobility services are provided to both wireless and wired stations.

The switch provides seamless roaming, which requires transparency of the network configuration and deployment options to the client.

From the end user's perspective, any mobility event must not change its IP address, its default router or DHCP server. This means that as stations roam, they must be able to

- Send an ARP to their default router, or
- Transmit a DHCP request to the server that had previously assigned their address.

From the infrastructure's perspective, as mobility events occur, the station's traffic must follow its current point of attachment, which can either be a mobility agent (MA) or mobility controller (MC). This must be true regardless of whether the station has moved to a network that is configured for a different subnet. The period from which the station is not receiving traffic following its mobility event must be as short as possible, even below 40 ms whenever possible, which includes any authentication procedures that are required.

From the infrastructure's perspective, the mobility management solution must have four main components, and all of these functions must be performed within the constraints of roaming:

- Initial Association—This function is used to identify the user's new point of attachment in the network.
- Context Transfer—This function is used to transfer state information associated with the station. This ensures that the station's static and real-time policies, including security and application ACLs, and services, remain the same across handoffs.

- Handoff—This function is used to signal that the station's point of attachment has changed, and control of the station should be relinquished by the previous access switch.
- Data Plane—This function is typically tied to the handoff process, and ensures that the station's traffic continues to be delivered and received from the station without any noticeable performance degradation.

Caution If you have configured virtual routing and forwarding (VRF) on wireless management interface VLAN, the mobility feature may not work expected.

Note You must enable PIM, IP ROUTING and IP MULTICAST Routing for wireless mobility multicast to work.

Wired and Wireless Mobility

One of the key features of the Converged access solution (applicable to both the Cisco Catalyst 3850 Switch and Cisco WLC 5700 Series Controller) is its ability to provide a device with an IP address and maintain its session persistence, across mobility events from ethernet connections to wireless and vice-versa. This feature allows users to remain on an ethernet network when possible, and make use of the freedom of mobility associated with wireless when necessary.

This feature leverages support from both the client and the infrastructure and uses the two factor authentication-device and user. The device authentication credentials is cached in the mobility controller (MC). When a device transitions across link layers, the device credentials is validated, and if a match is found, the MC ensures that the same IP address is assigned to the new interface.

Features of Mobility

- Mobility Controller (MC)—The controller provides mobility management services for inter-peer group roaming events. The MC provides a central point of contact for management and policy based control protocols, such as RADIUS. This eliminates the need for the infrastructure servers to maintain a user's location as it transitions throughout the network. The MC sends the configuration to all the mobility agents under its sub-domain of their mobility configuration, peer group membership and list of members. A sub-domain is synonymous to the MC that forms it. Each sub-domain consists of an MC and zero or more access switches that have AP's associated to them.
- Mobility Agents (MA)— A mobility agent is either an access switch that has a wireless module running on it or an MC with an internal MA running on it. A mobility agent is the wireless component that maintains client mobility state machine for a mobile client that is connected via an AP to the device that the MA is running on.
- Mobility Sub Domain— It is an autonomous portion of the mobility domain network. A mobility sub-domain comprises of a single mobility controller and its associated mobility agents (MAs).

Note Even when more than one mobility controller is present, only one MC can be active at any given time.

A mobility sub-domain is the set of devices managed by the active mobility controller. A mobility sub-domain comprises of a set of mobility agents and associated access points.

- Mobility Group— A collection of mobility controllers (MCs) across which fast roaming is supported. The concept of mobility group is the same as a collection of buildings in a campus across which frequent roaming is expected.
- Mobility Domain— A collection of mobility sub-domains across which mobility is supported. The term mobility domain may be the same as a campus network.
- Mobility Oracle (MO)—The mobility oracle acts as the point of contact for mobility events that occur across mobility sub-domains. It also maintains a local database of each station in the entire mobility domain, their home and current sub-domain. A mobility domain includes one or more mobility oracle, though only one would be active at any given time.
- Mobility Tunnel Endpoint (MTE)— The mobility tunnel endpoint (MTE) provides data plane services for mobile devices through the use of tunneling. This minimizes the impact of roaming events on the network by keeping the user's point of presence on the network a constant.
- Point of Attachment— A station's point of attachment is where its data path is initially processed upon entry in the network. This could either be the access switch that is currently providing it service, or the wireless LAN controller.
- Point of Presence— A station's point of presence is the place in the network where the station is being advertised. For instance, if an access switch is advertising reachability to the station via a routing protocol, the interface on which the route is being advertised is considered the station's point of presence.
- Switch Peer Group (SPG)— A peer group is a statically created list of neighboring access switches between which fast mobility services is provided. A peer group limits the scope of interactions between switches during handoffs to only those that are geographically proximate.
- Station—A user's device that connects to and requests service from the network. The device may have a wired, wireless or both interfaces.
- Switch in the same SPG—A peer switch that is part of the peer group of the local switch.
- Switch outside the SPG—A peer access switch that is not part of the local switch's peer group.
- Foreign Mobility Controller— The mobility controller providing mobility management service for the station in a foreign mobility sub-domain. The foreign mobility controller acts as a liaison between access switches in the foreign sub-domain and the mobility controller in the home domain.
- Foreign Mobility Sub-Domain— The mobility sub-domain, controlled by a mobility controller, supporting a station which is anchored in another mobility sub-domain
- Foreign Switch— The access switch in the foreign mobility sub-domain currently providing service to the station.
- Anchor Mobility Controller— The mobility controller providing a single point of control and mobility management service for stations in their home mobility sub-domain.

- Anchor Mobility Sub-Domain— The mobility sub-domain, controlled by a mobility controller, for a station where its IP address was assigned.
- Anchor Switch— The switch in the home mobility sub-domain that last provided service to a station.

Sticky Anchoring for Low Latency Roaming

Sticky Anchoring ensures low roaming latency from the client's point of presence is maintained at the switch where the client initially joins the network. It is expensive to apply client policies at a switch for a roaming client. There can be considerable delay as it involves contacting the AAA server for downloadable ACLs which is not acceptable for restoring time sensitive client traffic.

To manage this delay, when the client roams between APs connected to different switches , irrespective of whether it is an intra sub-domain roam or inter sub-domain roam, the client traffic is always tunneled to the switch where the client first associates. The client is anchored at its first point of attachment for its lifetime in the network.

This behavior is enabled by default. You can also disable this behavior to allow the client anchoring only for inter-subnet roams. This configuration is per WLAN config and is available under the WLAN config mode. The customer can configure different SSIDs for time sensitive and non time sensitive applications.

Bridge Domain ID and L2/L3 Roaming

Bridge domain ID provides the mobility nodes with information to decide on specific roam type, either as L2 or L3 roam. It also allows the network administrators to reuse the VLAN IDs across network distribution. When the VLAN IDs do not have the associated subnet configurations, they may require additional parameter to use in conjunction with VLAN ID. The network administrator ensures that the given VLAN under the same bridge domain ID are associated with the unique subnet. The mobility nodes will first check for the bridge domain ID for the given node and the VLAN ID associated with the client to identify the roam type. The bridge domain ID and the VLAN ID must be same to treat a roam as L2 roam.

The bridge domain ID is configured for each SPG when creating a SPG and later on the MC. The bridge domain ID could be same for more than one SPG and all the MAs under the SPG will share the same bridge domain ID. This information is pushed to the MAs as part of the configuration download when MA comes up initially. If the bridge domain ID is modified when the system is up, it will be pushed to all the MAs in the modified SPG and will take immediate effect for the future roams.

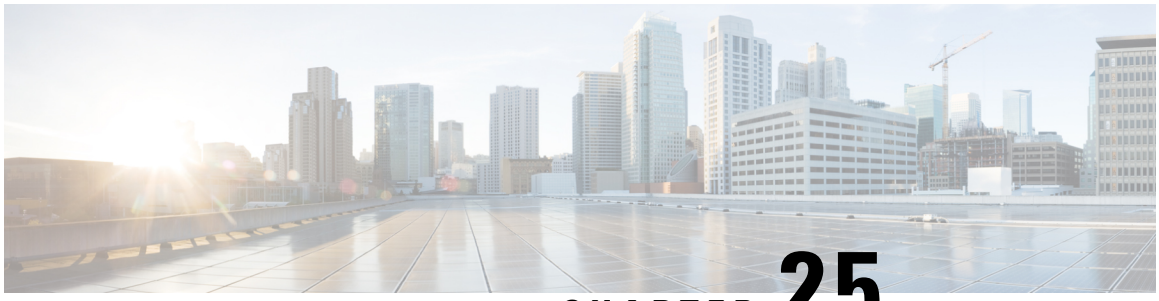
Link Down Behavior

This section provides information about data synchronization between MA-MC and MC-MO when MC or MO faces downtime in absence of redundancy manager. When Keepalive is configured between MA-MC or MC-MO the clients database is synchronized between the MO and the MCs and the MC and its MAs respectively.

Platform Specific Scale Requirement for the Mobility Controller

The Mobility Controller (MC) role is supported on a number of different platforms like, the Cisco WLC 5700 Series, CUWN and Catalyst 3850 Switches. The scale requirements on these three platforms are summarized in the table below:

Scalability	Catalyst 3850 as MC	Catalyst 3650 as MC	Cisco WLC 5700 as MC	CUWN 5508 as MC	WiSM2 as MC
Max number of MC in Mobility Domain	8	8	72	72	72
Max number of MC in Mobility Group	8	8	24	24	24
Max number of MAs in Sub-domain (per MC)	16	16	350	350	350
Max number of SPGs in Sub-domain (per MC)	8	8	24	24	24
Max number of MAs in a SPG	16	16	64	64	64



CHAPTER 25

Mobility Network Elements

Mobility Agent

- Handling the mobility events on the switch
- Configuring the datapath elements on the switch for mobility, and
- Communicating with the mobility controller

As MA, the switch performs the datapath functions by terminating the CAPWAP tunnels that encapsulate 802.11 traffic sourced by wireless stations.

This allows the switch to apply features to wired and wireless traffic in a uniform fashion. As far as switch is concerned, 802.11 is just another access medium.

The MA performs the following functions:

- Support the mobility protocol – The MA is responsible for responding in a timely manner, ensuring the switch is capable of achieving its roaming budget.
- Point of presence – If the wireless subnets are not available at the MC, the MA assumes the point of presence if the wireless client VLAN is not available at the new point of attachment and tunnel the client traffic accordingly.
- ARP Server – When the network is configured in a layer 2 mode, the MA is responsible for advertising reachability for the stations connected to it. If tunneling is employed, the ARP request is transmitted on behalf of the station through the tunnel, which the point of presence (anchor switch) would bridge onto its uplink interface.
- Proxy IGMP – The MA on the switch is responsible for subscribing to multicast groups on behalf of a station after a roaming event has occurred. This information is passed as part of the context to the new switch. This ensures the multicast flows follow the user as it roams.
- Routing – When the switch is connected to a layer 3 access network, the MA is responsible for injecting routes for the stations that are associated with it for which tunneling is not provided.
- 802.1X Authenticator – The authenticator function is included in the MA, and handles both wired and wireless stations.

- Secure PMK Sharing – When a station successfully authenticates to the network, the MA forwards the PMK to the MC. The MC is responsible for flooding the PMK to all the MAs under its sub-domain and to the peer MCs in the mobility group.

The MA also performs the following datapath functions:

- Mobility tunnel – If tunneling is used, the MA encapsulates and decapsulates packets from the mobility tunnel to the MC, and to other MA in the peer group, if the access switches are serving as points of presence. The MA supports the tunneling of client data traffic between the point of attachment and the point of attachment. The packet format used for other switches is CAPWAP with an 802.3 payload. The MA also supports reassembly and fragmentation for mobility tunnels.
- Encryption – The mobility control traffic between the mobility nodes is DTLS encrypted. The MA also encrypts the CAPWAP control and data (optional) at the point of attachment.
- CAPWAP – The switch supports the CAPWAP control and data planes. The switch forwarding logic is responsible for terminating the CAPWAP tunnels with 802.11 as well as 802.3 payloads. Since support for large frames (greater than 1500bytes) is not universally available, the switch supports CAPWAP fragmentation and reassembly.

Note Mobility tunnel path via an L3 interface on the 4500 or the L3 interface on the uplink port is not supported. It is not possible to have an L3 wireless management interface. Even if the tunnel comes up, packet forwarding is not possible as it is not supported. 4510 drops DHCP packets from wireless clients if SSID is anchored to a different Cisco WLC.

Mobility Controller

The main function of mobility controller is to coordinate the client roaming beyond a switch peer group. The other features of the mobility controller are:

- Station Database—The Mobility Controller maintains a database of all the clients that are connected within the local mobility sub-domain.
- Mobility Protocol—The MC supports the mobility protocol which ensures the target roaming point responds in a timely manner and achieves the 150ms roaming budget
- Interface to Mobility Oracle—The Mobility Controller acts as a gateway between the switch and the Mobility Oracle. When the Mobility Controller does not find a match in its local database, it suggests a match for a wireless client entry (in its database) and forwards the request to the Mobility Oracle, which manages the Mobility Domain.

Note Mobility Oracle function can be enabled on an MC only if it is supported by the platform.

- ARP Server—When tunneling is employed for a station, its point of presence on the network is the Mobility Tunnel Endpoint (MTE). The Mobility Controller responds to any ARP requests received for the stations it is responsible for.

- Configures MTE—The Mobility Controller is the control point for the switch for all mobility management related requests. When a change in a station's point of attachment occurs, the Mobility Controller is responsible for configuring the forwarding policy on the MTE.
- NTP Server—The Mobility Controller acts as an NTP server to the switch and supports all the nodes to have their clocks synchronized with it.

Note The Cisco 5700 series WLC and other controller platforms that have the Mobility Controller function enabled by default should not be added to a switch peer group (SPG).

Mobility Tunnel Endpoint

MTE is the Data plane component of MC and MA and provides data plane services for mobile devices through the use of tunneling .

The functions of the MTE include:

- Tunnel Termination: The MTE terminates the data part of mobility tunnels from the Switch. Traffic to and from the roamed client is sent to the foreign switch via the mobility tunnel.
- Inter-MTE Tunnel Termination – The MTE-MTE tunnel is used to tunnel traffic between mobility sub-domains. These tunnels have the same format as the Switch-MTE tunnels.
- Mobility Controller Configuration Interface: This is the interface the MC uses to configure the MTE's forwarding tables to reflect mobility events.

Mobility Oracle

The Mobility Oracle coordinates the client roams beyond the subdomain on a need basis and consists of the following features:

- Station Database—The Mobility Oracle maintains a database of all stations that are serviced within the mobility domain. This database is populated during the Mobility Oracle's interactions with all the Mobility Controllers, in all of the mobility sub-domains it supports.
- Interface to Mobility Controller—When the Mobility Oracle receives a request from a Mobility Controller, it performs a station lookup, and forwards, whenever needed, the request to the proper Mobility Controller.
- NTP Server—The Mobility Oracle acts as an NTP server to the Mobility Controllers and synchronizes all the **switch** clocks within the mobility domain.

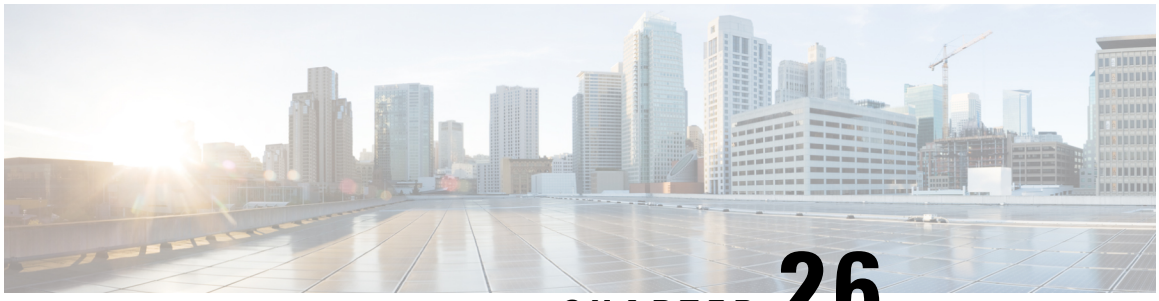
Guest Controller

The guest access feature provides guest access to wireless clients. The guest tunnels use the same format as the mobility tunnels. Using the guest access feature, there is no need to configure guest VLANs on the access switch. Traffic from the wired and wireless clients terminates on Guest Controller. Since the guest VLAN is not present on the access switch, the traffic is tunneled to the MTE over the existing mobility tunnel, and then via a guest tunnel to the Guest Controller.

The advantage of this approach is that all guest traffic passes through the MTE before it is tunneled to the Guest Controller. The Guest Controller only needs to support tunnels between itself and all the MTEs.

The disadvantage is that the traffic from the guest client is tunneled twice - once to the MTE and then again to the Guest Controller.

Clients cannot roam to Guest Controllers because roaming is not supported on Guest Controllers. This restriction is applicable only for the IOS-XE guest anchor, and not for AireOS.



CHAPTER 26

Mobility Control Protocols

About Mobility Control Protocols

The mobility control protocol is used regardless of whether tunneled or routed. The mobility control protocol is used for mobility events between the MO, MC and MA.

The mobility architecture uses both,

- Distributed approach, using the direct communication with the switches in their respective SPG, as well as
- Centralized approach, using the MC and MO.

The goal is to reduce the overhead on the centralized MC, while limiting the interactions between switches to help scale the overall system.

Initial Association and Roaming

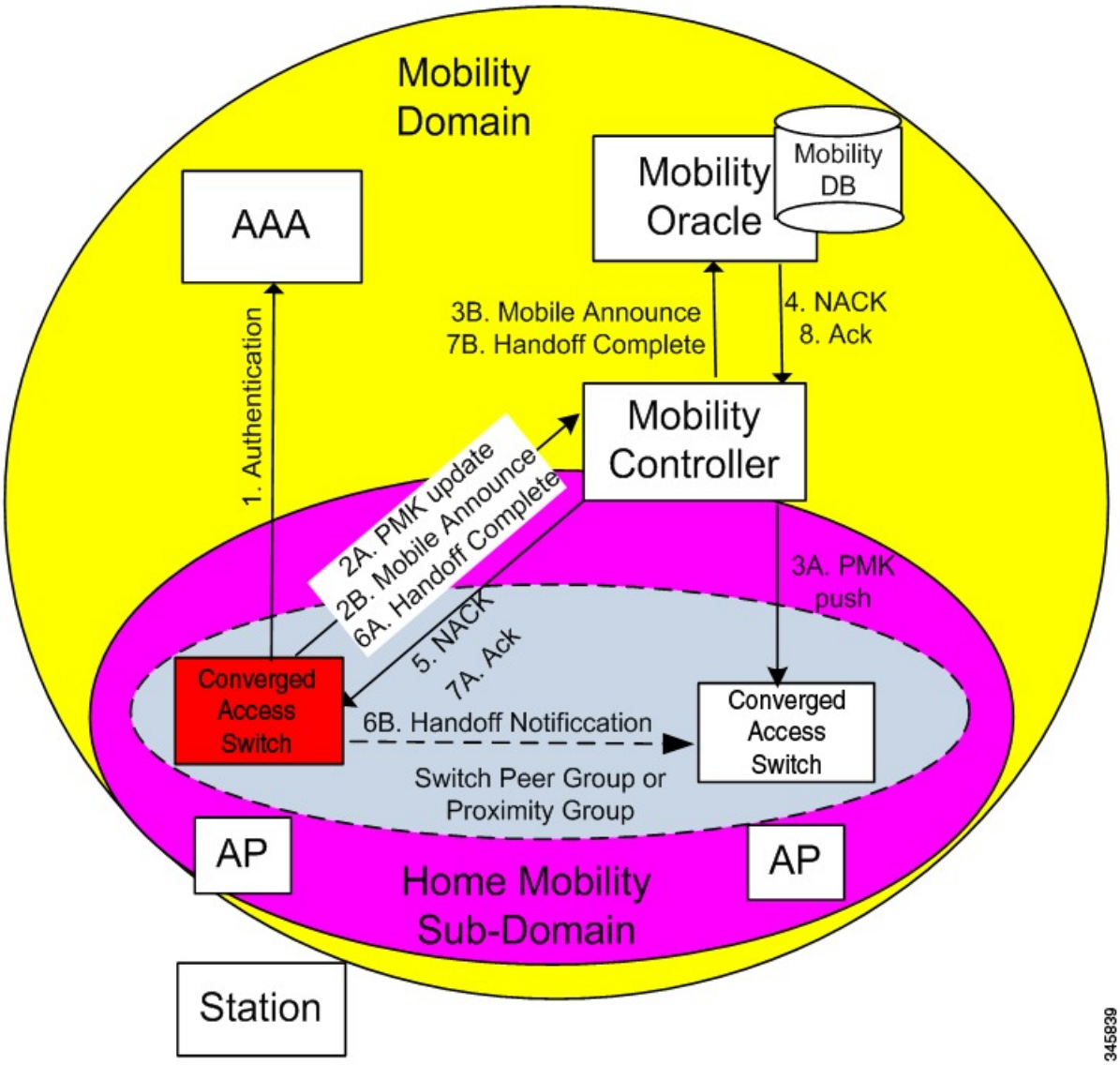
The following scenarios are applicable to the mobility management protocol:

- Initial Association
- Intra Switch Roam
- Intra Switch Peer Group Roam
- Inter Switch Peer Group Roam
- Inter Sub-Domain Roam
- Inter Group Roam

Initial Association

The illustration below explains the initial association process followed by theswitch:

Figure 21: Initial Association



1. When a station initially associates with a mobility agent, the MA performs a lookup to determine whether keying information for key caching is locally available in the MA. If no keying information is available, which is the case when the station first appears in the network, the switch prompts the device to authenticate itself to generate the Pairwise Master Key (PMK). The PMK is generated on the client and the RADIUS server side, and the RADIUS sever forwards the PMK to the authenticator, the MA.
2. The MA sends the PMK to the MC.
3. After receiving the PMK from the MA, the MC transmits the PMK to all the MAs in its sub-domain, and to all the other MCs in its mobility group.

4. The mobility group is a single key domain. This ensures that 802.11r compliant stations recognize the key domain, and attempts to utilize the fast transition procedures defined in 802.11r.

Note The 802.11r protocol defines a key domain, which is a collection of access points that share keying information.

5. (Refer to step 2B in the illustration). Since the station is new to the mobility sub-domain, as indicated by the fact that the PMK is not in the MA local key cache, the MA transmits a mobile announce message to the MC.
6. The MC checks if the client exists in its database. As the client cannot be found, the MC in turn forwards it to the MO, if available.
7. (Refer to step 5 in the illustration). As the station is new to the network, the MO returns a negative response (NACK), which is forwarded by the MC to the switch. If the Mobility Oracle is not available then the MC is responsible for not responding to the Mobile Announce.

Note In new mobility if there are many peers, the IOS controller will not react on a NACK message from the AirOS peer and sends two more probes. NACK is ignored if the client is not present it just drops it, is such a scenario AIREOS sends the NACK. So NACK from mobility controller is not processed.

8. The MA on the switch informs the MC about the station's new point of attachment via the Handoff Complete message.
9. The MA then informs the other MAs in its switch peer group (SPG) about the station's new point of attachment via the Handoff Notification message. It is necessary to transmit this notification to the MAs in its SPG to allow local handoff without interacting with the MC. The Handoff Notification message sent to MAs in SPG need not carry all the information in Handoff Complete message sent to the MC.
10. (Refer to step 7B in the illustration). The MC updates its database and forwards the Handoff Complete message to the Mobility Oracle. This ensures that the Mobility Oracle's database is updated to record the station's current home mobility sub-domain.

To eliminate race conditions that could occur with devices moving quickly across switch, regardless of whether they are within a mobility sub-domain or not, the messages between MA and MC/MO are time synchronized. This would allow the MC and MO to properly process requests, if they are received out of order.

The Handoff Notification sent to MAs in the SPG are not acknowledged.

Intra Switch Handoff

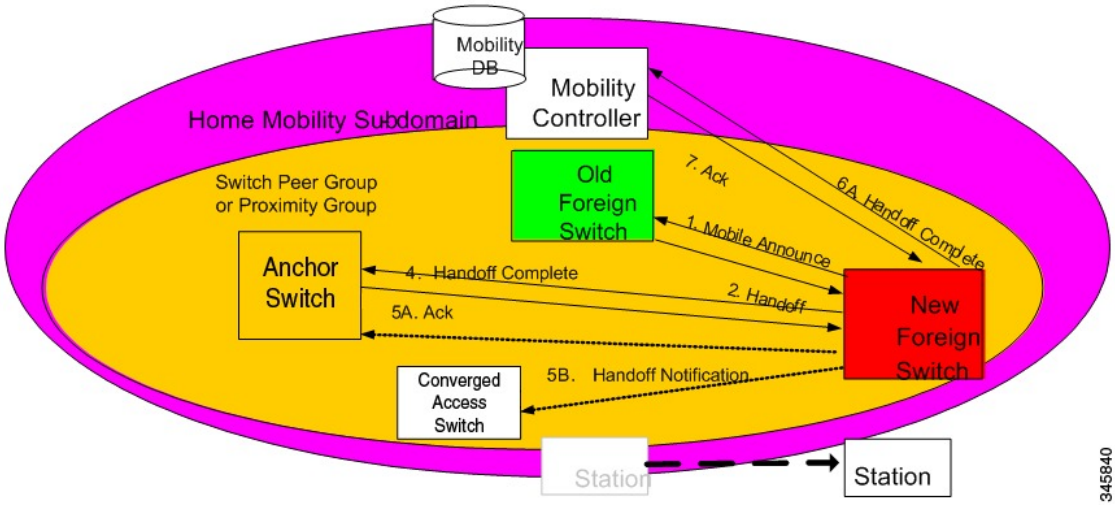
Mobility events within an MA are completely transparent to the SPG and the MC. When a station moves across APs on the same MA and attempts to perform a fast handoff, the PMK is present on the MA. The MA will complete the fast handoff without invoking any additional signal.

Intra Switch Peer Group Handoff

The switch peer group (SPG) is a group of MAs between which users may roam, and expect fast roaming services. Allowing the MA to handoff directly within a SPG reduces the overhead on the MC as it requires fewer messages to be exchanged.

After the initial association is complete the station moves to another MA belonging to its SPG. In an intra switch peer group roam, the initial association, the stations PMK was forwarded to all MAs in the mobility sub-domain.

Figure 22: Intra Switch Peer Group Handoff



The following process explains the intra switch peer group handoff:

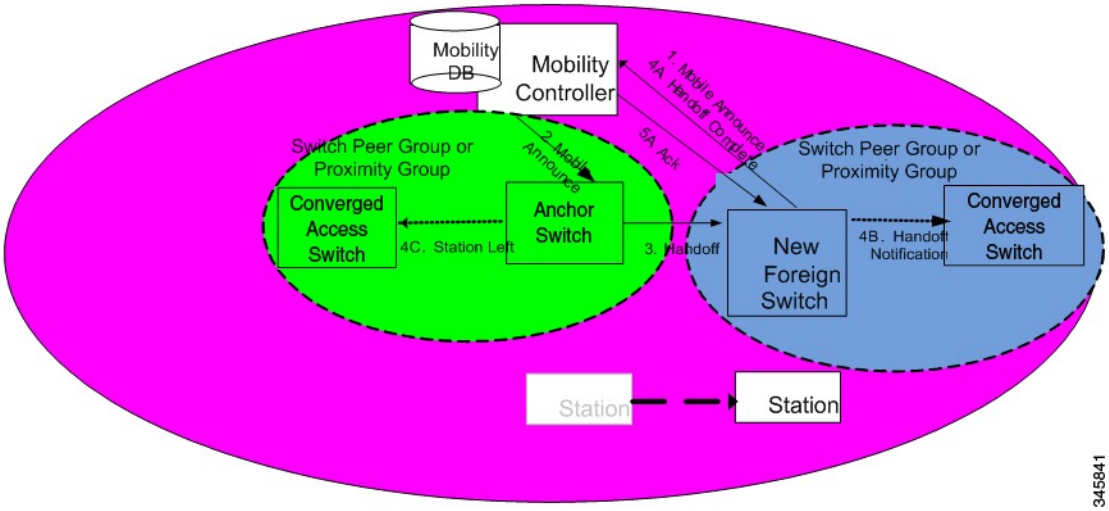
1. In the initial association example, the Handoff Notification message is sent to all MAs in its SPG to know the station's current point of attachment.
2. The new MA sends a unicast Mobile Announce message to the previous MA to which the client is associated.
3. After the handoff completion, the new MA transmits a Handoff Complete message to the MC.
4. The new switch sends a Handoff Notification to all MA in its own SPG to inform them about the clients new point of presence.

Inter Switch Peer Group Handoff

The Intra SPG roams do not cover all possible scenarios and there can be cases where it is possible for mobility events to occur between two MAs that are not in the same SPG.

When a MA does not have any information about a station's current point of attachment, because of the Handoff Notification message getting lost in the network, or because of the the station roaming to an MA that is not in the new SPG, the MA consults the MC. The MC provides information about the clients point of presence within the mobility sub-domain. This eliminates the need to consult all other MCs within the mobility sub-domain.

Figure 23: Inter Switch Peer Group Handoff



The image above illustrates an example of a mobility event that occurs across MAs that are not in the same SPG, but within the same mobility sub-domain.

Note The MA color matches the circle representing its SPG.

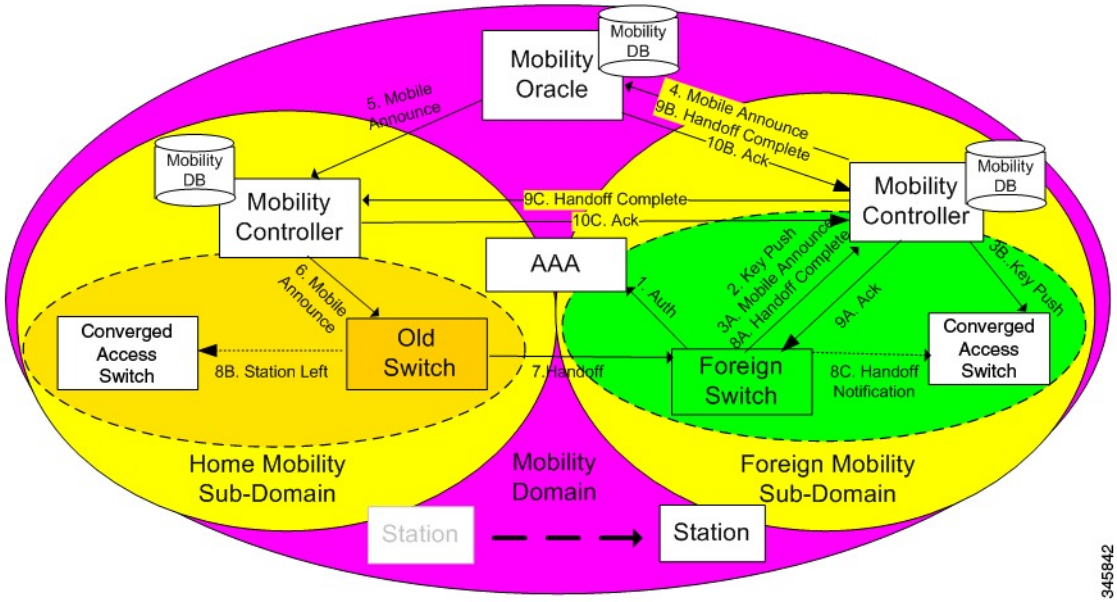
1. The new MA will have the PMK for the station, which was forwarded to each MA in the mobility sub-domain upon client initial authentication.
2. Since the MA had not been previously notified of the station's presence on a neighboring MA inside a different SPG transmits the mobile announce to the sub-domain's MC.
3. (Refer to step 2 in the illustration) On receiving the mobile announce message, the MC performs a lookup in its database, and forwards the request to the MA that was previously providing service to the station. This information is known to the MC through a previously received Handoff Complete message sent in a reliable fashion from the old MA.
4. (Refer to step 3 in the illustration) The old MA, shown in green above, transmits a Handoff message directly to the new MA.
5. The old MA needs to notify other MAs within its SPG of the fact that the station has left the group using a Station Left message. This ensures that if the station were to come back to one of the MA , they would be aware of the fact that the station is no longer being serviced by the old MA.
6. Once the handoff is complete, the new MA transmits the Handoff Complete message in a reliable fashion to the MC.
7. The new MA then transmits the Handoff Notification to the other MAs within its SPG.

Inter Sub Domain Handoff

A sub-domain is an ensemble formed by a mobility controller and the mobility agents it directly manages. An inter sub-domain mobility event implies communication between two mobility controllers. These 2 mobility controllers can be configured with the same mobility group value and recognize each other. They will appear in each other's mobility list, or they can be configured with different mobility group values, and still recognize each other.

When the roaming event occurs across sub-domains between MCs in the same mobility group, the 802.11r key domain advertised by the new APs are the same. Additionally, the client PMK is also transmitted to all MCs upon the client's initial authentication. The new MC does not need to force the client to reauthenticate, and the new MC also knows which previous MC was managing the wireless client mobility.

Figure 24: Inter Sub Domain Handoff



The following steps are involved in the inter sub domain handoff, when mobility controllers belong to the same mobility group:

1. When a clients PMK was sent by the initial MA to all the MCs in the mobility group, the new MA already had already received the client PMK from its MC, and re-authentication is not required.
2. The new MA was not notified previously of the station's presence on a neighboring MA inside a different SPG it transmits the mobile announce to the sub-domain's MC.
3. On receiving the mobile announce message, the MC forwards the mobile announce to the MO, which performs a lookup in its database, and forwards the request to the MC that was previously providing service to the station.
4. The previous MC, in turn, forwards the request to the MA that was previously providing service to the station.
5. The old MA, shown in yellow color above, transmits a Handoff message directly to the new MA.
6. The old MA must notify the other MAs within its SPG of the fact that the station has left the SPG using a Station Left message. This ensures that if the station comes back to one of the MA , the MA is aware of the fact that the station is no longer serviced by the old MA.
7. Once the handoff is complete, the new MA transmits the Handoff Complete message in a reliable fashion to the new Mobility Controller.
8. The new MA then transmits the Handoff Notification to all other MAs.
9. The new MC then transmits the Handoff Complete to the old MC.

Inter Mobility Group Handoff

A mobility group is formed by MCs sharing the same mobility group name, and knowing each other.

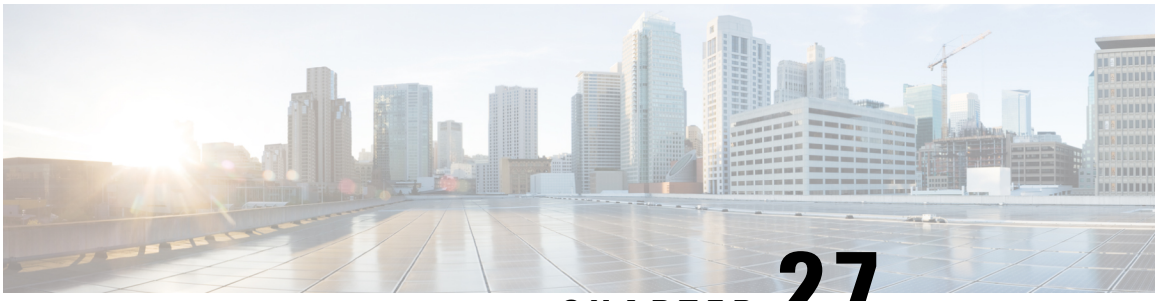
Since the roaming event occurs across mobility groups, the 802.11r key domain advertised by the new APs differ. This forces the client to re-authenticate. They are propagated only within a mobility group, and roaming across mobility groups requires the stations to re-authenticate when they cross mobility group boundaries. When the authentication is complete, the PMK that is generated is pushed to the MAs and MCs within the same mobility group. The stations cache the PMK from the previous sub-domain because each PMK is associated to a given sub-domain (802.11y key domain). This ensures that you do not have to re-authenticate when the PMK roams back to the previous sub-domain within the pmk cache timeout interval. The remaining procedure follows the inter-sub-domain handoff steps, except that these steps relate to inter mobility group roaming.

Three Way Sub Domain Handoff

The also supports mobility events that occur across foreign domains, known as a three-way sub-domain mobility event.

The illustration below explains the interaction between the Mobility Controllers in both foreign sub-domains through the Mobility Oracle.

The message exchange shown in the illustration is identical to that described in Inter Sub Domain Handoff except for the exception that the Handoff Complete notification is transmitted to the Mobility Controllers in the old foreign sub-domain as well as the home sub-domain.



CHAPTER 27

Configuring Mobility

Configuring Mobility Controller

Configuring Converged Access Controllers

Creating Peer Groups, Peer Group Member, and Bridge Domain ID (CLI)

Before you begin

- On the mobility agent, you can only configure the IP address of the mobility controller.
- On the mobility controller, you can define the peer group and the IP address of each peer group member.

Procedure

	Command or Action	Purpose
Step 1	**wireless mobility controller** **Example:** `Switch(config)# wireless mobility controller`	Enables the mobility controller functionality on the device. This command is applicable only to the switch. The controller is by default a mobility controller.
Step 2	**wireless mobility controller peer-group** *SPG1* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1`	Creates a peer group named SPG1.

	Command or Action	Purpose
Step 3	**wireless mobility controller peer-group** *SPG1* **member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.2 public-ip 10.10.20.2`	Adds a mobility agent to the peer group. **Note** The `10.10.20.2` is the mobility agent's direct IP address. When NAT is used, use the optional public IP address to enter the mobility agent's NATed address. When NAT is not used, the public IP address is not used and the device displays the mobility agent's direct IP address.
Step 4	**wireless mobility controller peer-group** *SPG1* **member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6 public-ip 10.10.20.6`	Adds another member to the peer group SPG1.
Step 5	**wireless mobility controller peer-group** *SPG2* **Example:** `Switch(config)# wireless mobility controller peer-group SPG2`	Creates another peer group SPG2.
Step 6	**wireless mobility controller peer-group** *SPG2* **member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility controller peer-group SPG2 member ip 10.10.10.20 public-ip 10.10.10.20`	Adds a member to peer group SPG2.
Step 7	**wireless mobility controller peer-group** *SPG1* **bridge-domain-id** *id* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1 bridge-domain-id 54`	(Optional) Adds a bridge domain to SPG1 used for defining the subnet-VLAN mapping with other SPGs.

Example

This example shows how to create peer group and add members to it:

```
Switch(config)# wireless mobility controller
Switch(config)# wireless mobility controller peer-group SPG1
Switch(config)# wireless mobility controller peer-group SPG1
Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.2 public-ip
```

```
 10.10.20.2
Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6 public-ip
 10.10.20.6
Switch(config)# wireless mobility controller peer-group SPG2
Switch(config)# wireless mobility controller peer-group SPG2 member ip 10.10.10.20 public-ip
 10.10.10.20
Switch(config)# wireless mobility controller peer-group SPG1 bridge-domain-id 54
```

Creating Peer Groups, Peer Group Member, and Bridge Domain ID (GUI)

Before you begin

- Ensure that the device is in mobility controller state.
- On the mobility agent, you can only configure the IP address of the mobility controller.
- On the mobility controller, you can define the peer group and the IP address of each peer group member.

Procedure

Step 1 Choose **Controller** > **Mobility Management** > **Switch Peer Group**.

The **Mobility Switch Peer Groups** page is displayed.

Step 2 Click **New**.

Step 3 Enter the following details:

a) **Switch Peer Group Name**
b) **Bridge Domain ID**
c) **Multicast IP Address**

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Configuring Optional Parameters for Roaming Behavior

Use this configuration to disable the sticky anchor. This command can also be used, if required, between all MA's and MC's where roaming is expected for the target SSID.

Procedure

	Command or Action	Purpose
Step 1	**wlan open21** **Example:** `Switch(config)# wlan open20`	Configures a WLAN.
Step 2	**no mobility anchor sticky** **Example:**	Disables the default sticky mobility anchor.

	Command or Action	Purpose
	`Switch(config-wlan)# no mobility anchor sticky`	

Example

```
Switch(config)# wlan open20
Switch(config-wlan)# no mobility anchor sticky
```

Configuring Local Mobility Group (CLI)

Configuration for wireless mobility groups and mobility group members where the mobility group is a group of MCs.

Before you begin

MCs can belong only to one mobility group, and can know MCs in several mobility groups.

Procedure

	Command or Action	Purpose
Step 1	**wireless mobility group name** *group-name* **Example:** `Switch(config)# wireless mobility group name Mygroup`	Creates a mobility group named **Mygroup**.
Step 2	**wireless mobility group member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility group member ip 10.10.34.10 public-ip 10.10.34.28`	Adds a mobility controller to the **Mygroup** mobility group. **Note** When NAT is used, use the optional public IP address to enter the NATed IP address of the mobility controller.
Step 3	**wireless mobility group keepalive interval** *time-in-seconds* **Example:** `Switch(config)# wireless mobility group keepalive interval 5`	Configures the interval between two keepalives sent to a mobility member.
Step 4	**wireless mobility group keepalive count** *count* **Example:** `Switch(config)# wireless mobility group keepalive count 3`	Configures the keep alive retries before a member status is termed DOWN.

Example

```
Switch(config)# wireless mobility group name Mygroup
Switch(config)# wireless mobility group member ip 10.10.34.10 public-ip 10.10.34.28
Switch(config)# wireless mobility group keepalive interval 5
Switch(config)# wireless mobility group keepalive count 3
```

Configuring Local Mobility Group (GUI)

Before you begin

Mobility controllers can belong to only one mobility group and can know mobility controllers in several mobility groups.

Procedure

Step 1 Choose **Controller** > **Mobility Management** > **Mobility Global Config**.

The **Mobility Controller Configuration** page is displayed.

Step 2 Enter the following details:

a) **Mobility Group Name**
b) **Mobility Keepalive Interval**
c) **Mobility Keepalive Count**
d) **Multicast IP Address** if you want to enable multicast mode to send mobile announce messages to the mobility members.

Note If you do not enable multicast IP address, the device uses unicast mode to send mobile announce messages.

Step 3 Click **Apply**.

Step 4 Click **Save Configuration**.

Adding a Peer Mobility Group (CLI)

Before you begin

MCs belong to only one group, and can know MCs in several groups.

Procedure

	Command or Action	Purpose
Step 1	**wireless mobility group member ip** *member-ip-addr* **public-ip** *public-ip-addr* **group** *group-name* **Example:**	Adds the member as a peer MC in a different group than the **Mygroup**.

	Command or Action	Purpose
	`Switch(config)# wireless mobility group member ip 10.10.10.24 public-ip 10.10.10.25 group Group2`	

Adding a Peer Mobility Group (GUI)

Before you begin

Mobility controllers belong to only one group, and can know several mobility groups.

Procedure

Step 1 Choose **Controller** > **Mobility Management** > **Mobility Peer**.

The **Mobility Peer** page is displayed.

Step 2 Click **New**.

Step 3 Enter the following details:

a) **Mobility Member IP**
b) **Mobility Member Public IP**
c) **Mobility Member Group Name**
d) **Multicast IP Address**

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Configuring Optional Parameters for Roaming Behavior

Use this configuration to disable the sticky anchor. This command can also be used, if required, between all MA's and MC's where roaming is expected for the target SSID.

Procedure

	Command or Action	Purpose
Step 1	**wlan open21** **Example:** `Switch(config)# wlan open20`	Configures a WLAN.
Step 2	**no mobility anchor sticky** **Example:** `Switch(config-wlan)# no mobility anchor sticky`	Disables the default sticky mobility anchor.

Example

```
Switch(config)# wlan open20
Switch(config-wlan)# no mobility anchor sticky
```

Pointing the Mobility Controller to a Mobility Oracle (CLI)

Before you begin

You can configure a mobility oracle on a known mobility controller.

Procedure

	Command or Action	Purpose
Step 1	**wireless mobility group member ip** *member-ip-addr* **group** *group-name* **Example:** `Switch(config)# wireless mobility group member ip 10.10.10.10 group Group3`	Creates and adds a MC to a mobility group.
Step 2	**wireless mobility oracle ip** *oracle-ip-addr* **Example:** `Switch(config)# wireless mobility oracle ip 10.10.10.10`	Configures the mobility controller as mobility oracle.

Example

```
Switch(config)# wireless mobility group member ip 10.10.10.10 group Group3
Switch(config)# wireless mobility oracle ip 10.10.10.10
```

Pointing the Mobility Controller to a Mobility Oracle (GUI)

Before you begin

You can configure a mobility oracle on a known mobility controller.

Procedure

Step 1 Choose **Controller** > **Mobility Management** > **Mobility Global Config**.

The **Mobility Controller Configuration** page is displayed.

Step 2 Enter the **Mobility Oracle IP Address**.

Note To make the mobility controller itself a mobility oracle, select the **Mobility Oracle Enabled** check box.

Step 3 Click **Apply**.

Step 4 Click **Save Configuration**.

Configuring Guest Controller

A guest controller is used when the client traffic is tunneled to a guest anchor controller in the demilitarized zone (DMZ). The guest client goes through a web authentication process. The web authentication process is optional, and the guest is allowed to pass traffic without authentication too.

Enable the WLAN on the mobility agent on which the guest client connects with the mobility anchor address of the guest controller.

On the guest controller WLAN, which can be Cisco 5500 Series WLC, Cisco WiSM2, or Cisco 5700 Series WLC, configure the IP address of the mobility anchor as its own IP address. This allows the traffic to be tunneled to the guest controller from the mobility agent.

Note With Cisco 5700 Series WLC as the guest anchor controller and Cisco 5500 Series WLC or Cisco WiSM2 as export foreign controller, the guest user role per user is not supported on the Cisco 5700 Series WLC.

Procedure

	Command or Action	Purpose
Step 1	**wlan** *wlan-id* **Example:** `Switch(config)# wlan Mywlan1`	Creates a WLAN for the client.
Step 2	**mobility anchor** *guest-anchor-ip-addr* **Example:** `Switch(config-wlan)# mobility anchor 10.10.10.2`	Enables the guest anchors (GA) IP address on the MA. **Note** To enable guest anchor on the mobility controller, you need not enter the IP address. Enter the **mobility anchor** command in the WLAN configuration mode to enable GA on the mobility controller.
Step 3	**client vlan** *vlan-name* **Example:** `Switch(config-wlan)# client vlan gc_ga_vlan1`	Assigns a VLAN to the client's WLAN.
Step 4	**security open** **Example:** `Switch(config-wlan)# security open`	Assigns a security type to the WLAN.

Example

```
Switch(config)# wlan Mywlan1
Switch(config-wlan)# mobility anchor 10.10.10.2
Switch(config-wlan)# client vlan gc_ga_vlan1
Switch(config-wlan)# security open
```

Configuring Guest Anchor

Procedure

	Command or Action	Purpose
Step 1	**wlan Mywlan1** **Example:** `Switch(config)# wlan Mywlan1`	Creates a wlan for the client.
Step 2	**mobility anchor <guest-anchors-own-ip-address>** **Example:** `Switch(config-wlan)# mobility anchor 10.10.10.2`	Enables the guest anchors IP address on the guest anchor (GA). The GA assigns its own address on itself.
Step 3	**client vlan<vlan-name>** **Example:** `Switch(config-wlan)# client vlan gc_ga_vlan1`	Assigns a vlan to the clients wlan.
Step 4	**security open** **Example:** `Switch(config-wlan)# security open`	Assigns a security type to the wlan.

Example

```
Switch(config)# wlan Mywlan1
Switch(config-wlan)# mobility anchor 10.10.10.2
Switch(config-wlan)# client vlan gc_ga_vlan1
Switch(config-wlan)# security open
```

Configuring Converged Access Controller on 5508 or WiSM 2

Enabling the New Mobility

Before you begin

You will require Cisco Unified Wireless Network 7.3 MR1, 8.0 or later to configure the new mobility architecture.

Procedure

	Command or Action	Purpose
Step 1	**config mobility new-architecture enable** **Example:** `(Cisco Controller) >config mobility new-architecture enable`	Enables and installs the new mobility architecture on the CUWN based controller.

Example

```
(Cisco Controller) >config mobility new-architecture enable
Enabling new-architecture would change mobility architecture from flat to hierarchical !!!
Configuration changes will be saved and System will be rebooted. !!!
Are you sure you want to continue? (y/n) y
```

Configuring Mobility Controller

This configuration shows how to change the MCs public address, or mobility group name.

Procedure

	Command or Action	Purpose
Step 1	**Example:**	

Example

Creating Peer Groups, Peer Group Member, and Bridge Domain ID (CLI)

Before you begin

- On the mobility agent, you can only configure the IP address of the mobility controller.
- On the mobility controller, you can define the peer group and the IP address of each peer group member.

Procedure

	Command or Action	Purpose
Step 1	**wireless mobility controller** **Example:** `Switch(config)# wireless mobility controller`	Enables the mobility controller functionality on the device. This command is applicable only to the switch. The controller is by default a mobility controller.
Step 2	**wireless mobility controller peer-group** *SPG1* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1`	Creates a peer group named SPG1.
Step 3	**wireless mobility controller peer-group** *SPG1* **member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.2 public-ip 10.10.20.2`	Adds a mobility agent to the peer group. **Note** The `10.10.20.2` is the mobility agent's direct IP address. When NAT is used, use the optional public IP address to enter the mobility agent's NATed address. When NAT is not used, the public IP address is not used and the device displays the mobility agent's direct IP address.
Step 4	**wireless mobility controller peer-group** *SPG1* **member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6 public-ip 10.10.20.6`	Adds another member to the peer group SPG1.
Step 5	**wireless mobility controller peer-group** *SPG2* **Example:** `Switch(config)# wireless mobility controller peer-group SPG2`	Creates another peer group SPG2.
Step 6	**wireless mobility controller peer-group** *SPG2* **member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility controller peer-group SPG2 member ip 10.10.10.20 public-ip 10.10.10.20`	Adds a member to peer group SPG2.
Step 7	**wireless mobility controller peer-group** *SPG1* **bridge-domain-id** *id* **Example:**	(Optional) Adds a bridge domain to SPG1 used for defining the subnet-VLAN mapping with other SPGs.

	Command or Action	Purpose
	`Switch(config)# wireless mobility controller peer-group SPG1 bridge-domain-id 54`	

Example

This example shows how to create peer group and add members to it:

```
Switch(config)# wireless mobility controller
Switch(config)# wireless mobility controller peer-group SPG1
Switch(config)# wireless mobility controller peer-group SPG1
Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.2 public-ip
 10.10.20.2
Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6 public-ip
 10.10.20.6
Switch(config)# wireless mobility controller peer-group SPG2
Switch(config)# wireless mobility controller peer-group SPG2 member ip 10.10.10.20 public-ip
 10.10.10.20
Switch(config)# wireless mobility controller peer-group SPG1 bridge-domain-id 54
```

Configuring Local Mobility Group (CLI)

Configuration for wireless mobility groups and mobility group members where the mobility group is a group of MCs.

Before you begin

MCs can belong only to one mobility group, and can know MCs in several mobility groups.

Procedure

	Command or Action	Purpose
Step 1	**wireless mobility group name** *group-name* **Example:** `Switch(config)# wireless mobility group name Mygroup`	Creates a mobility group named **Mygroup**.
Step 2	**wireless mobility group member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility group member ip 10.10.34.10 public-ip 10.10.34.28`	Adds a mobility controller to the **Mygroup** mobility group. **Note** When NAT is used, use the optional public IP address to enter the NATed IP address of the mobility controller.
Step 3	**wireless mobility group keepalive interval** *time-in-seconds* **Example:** `Switch(config)# wireless mobility group keepalive interval 5`	Configures the interval between two keepalives sent to a mobility member.

	Command or Action	Purpose
Step 4	**wireless mobility group keepalive count** *count* **Example:** `Switch(config)# wireless mobility group keepalive count 3`	Configures the keep alive retries before a member status is termed DOWN.

Example

```
Switch(config)# wireless mobility group name Mygroup
Switch(config)# wireless mobility group member ip 10.10.34.10 public-ip 10.10.34.28
Switch(config)# wireless mobility group keepalive interval 5
Switch(config)# wireless mobility group keepalive count 3
```

Adding a Peer Mobility Group (CLI)

Before you begin

MCs belong to only one group, and can know MCs in several groups.

Procedure

	Command or Action	Purpose
Step 1	**wireless mobility group member ip** *member-ip-addr* **public-ip** *public-ip-addr* **group** *group-name* **Example:** `Switch(config)# wireless mobility group member ip 10.10.10.24 public-ip 10.10.10.25 group Group2`	Adds the member as a peer MC in a different group than the **Mygroup**.

Configuring Optional Parameters for Roaming Behavior

Use this configuration to disable the sticky anchor. This command can also be used, if required, between all MA's and MC's where roaming is expected for the target SSID.

Procedure

	Command or Action	Purpose
Step 1	**wlan open21** **Example:** `Switch(config)# wlan open20`	Configures a WLAN.
Step 2	**no mobility anchor sticky** **Example:**	Disables the default sticky mobility anchor.

	Command or Action	Purpose
	`Switch(config-wlan)# no mobility anchor sticky`	

Example

```
Switch(config)# wlan open20
Switch(config-wlan)# no mobility anchor sticky
```

Pointing the Mobility Controller to a Mobility Oracle (CLI)

Before you begin

You can configure a mobility oracle on a known mobility controller.

Procedure

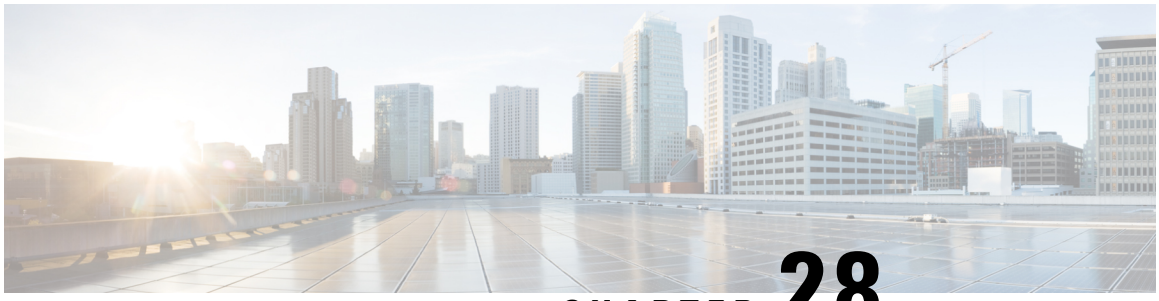
	Command or Action	Purpose
Step 1	**wireless mobility group member ip** *member-ip-addr* **group** *group-name* **Example:** `Switch(config)# wireless mobility group member ip 10.10.10.10 group Group3`	Creates and adds a MC to a mobility group.
Step 2	**wireless mobility oracle ip** *oracle-ip-addr* **Example:** `Switch(config)# wireless mobility oracle ip 10.10.10.10`	Configures the mobility controller as mobility oracle.

Example

```
Switch(config)# wireless mobility group member ip 10.10.10.10 group Group3
Switch(config)# wireless mobility oracle ip 10.10.10.10
```

PART VII

Multicast



CHAPTER 28

Configuring IGMP

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IGMP and IGMP Snooping

Prerequisites for IGMP

- Before performing the tasks in this module, you should be familiar with the concepts explained in the "IP Multicast Routing Technology Overview" module.
- The tasks in this module assume that IP multicast has been enabled and that the Protocol Independent Multicast (PIM) interfaces have been configured using the tasks described in the "Configuring Basic IP Multicast Routing" module.

Prerequisites for IGMP Snooping

Observe these guidelines when configuring the IGMP snooping querier:

- Configure the VLAN in global configuration mode.
- Configure an IP address on the VLAN interface. When enabled, the IGMP snooping querier uses the IP address as the query source address.
- If there is no IP address configured on the VLAN interface, the IGMP snooping querier tries to use the configured global IP address for the IGMP querier. If there is no global IP address specified, the IGMP querier tries to use the VLAN switch virtual interface (SVI) IP address (if one exists). If there is no SVI IP address, the switch uses the first available IP address configured on the switch. The first IP address available appears in the output of the **show ip interface** privileged EXEC command. The IGMP snooping querier does not generate an IGMP general query if it cannot find an available IP address on the switch.
- The IGMP snooping querier supports IGMP Versions 1 and 2.
- When administratively enabled, the IGMP snooping querier moves to the nonquerier state if it detects the presence of a multicast router in the network.
- When it is administratively enabled, the IGMP snooping querier moves to the operationally disabled state under these conditions:
  - IGMP snooping is disabled in the VLAN.
  - PIM is enabled on the SVI of the corresponding VLAN.

Restrictions for IGMP and IGMP Snooping

Restrictions for Configuring IGMP

The following are the restrictions for configuring IGMP:

- The switch supports IGMP Versions 1, 2 , and 3.

Note For IGMP Version 3, only IGMP Version 3 BISS (Basic IGMPv3 Snooping Support) is supported.

- IGMP Version 3 uses new membership report messages that might not be correctly recognized by older IGMP snooping switches.
- IGMPv3 can operate with both ISM and SSM. In ISM, both exclude and include mode reports are applicable. In SSM, only include mode reports are accepted by the last-hop router. Exclude mode reports are ignored.
- IGMP filtering and throttling is not supported under the WLAN.
- You cannot have a switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches.

Related Topics

Changing the IGMP Version(CLI), on page 331
IGMP Versions, on page 318

Restrictions for IGMP Snooping

The following are the restrictions for IGMP snooping:

- The switch supports IGMPv3 snooping based only on the destination multicast IP address. It does not support snooping based on a source IP address or proxy report.
- IGMPv3 join and leave messages are not supported on switches running IGMP filtering or Multicast VLAN registration (MVR).
- IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.
- The IGMP configurable leave time is only supported on hosts running IGMP Version 2. IGMP version 2 is the default version for the switch.

  The actual leave latency in the network is usually the configured leave time. However, the leave time might vary around the configured time, depending on real-time CPU load conditions, network delays and the amount of traffic sent through the interface.
- The IGMP throttling action restriction can be applied only to Layer 2 ports. You can use **ip igmp max-groups action replace** interface configuration command on a logical EtherChannel interface but cannot use it on ports that belong to an EtherChannel port group.

  When the maximum group limitation is set to the default (no maximum), entering the **ip igmp max-groups action** {**deny** | **replace**} command has no effect.

  If you configure the throttling action and set the maximum group limitation after an interface has added multicast entries to the forwarding table, the forwarding-table entries are either aged out or removed, depending on the throttling action.

Related Topics

Changing the IGMP Version(CLI), on page 331
IGMP Versions, on page 318

Information About IGMP

Role of the Internet Group Management Protocol

IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Enabling PIM on an interface also enables IGMP. IGMP provides a means to automatically control and limit the flow of multicast traffic throughout your network with the use of special multicast queriers and hosts.

- A querier is a network device, such as a router, that sends query messages to discover which network devices are members of a given multicast group.
- A host is a receiver, including routers, that sends report messages (in response to query messages) to inform the querier of a host membership. Hosts use IGMP messages to join and leave multicast groups.

Hosts identify group memberships by sending IGMP messages to their local multicast device. Under IGMP, devices listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a particular subnet.

IGMP Multicast Addresses

IP multicast traffic uses group addresses, which are Class D IP addresses. The high-order four bits of a Class D address are 1110. Therefore, host group addresses can be in the range 224.0.0.0 to 239.255.255.255.

Multicast addresses in the range 224.0.0.0 to 224.0.0.255 are reserved for use by routing protocols and other network control traffic. The address 224.0.0.0 is guaranteed not to be assigned to any group.

IGMP packets are transmitted using IP multicast group addresses as follows:

- IGMP general queries are destined to the address 224.0.0.1 (all systems on a subnet).
- IGMP group-specific queries are destined to the group IP address for which the device is querying.
- IGMP group membership reports are destined to the group IP address for which the device is reporting.
- IGMPv2 leave-group messages are destined to the address 224.0.0.2 (all devices on a subnet).
- IGMPv3 membership reports are destined to the address 224.0.0.22; all IGMPv3-capable multicast devices must listen to this address.

Related Topics

Configuring the Switch as a Member of a Group (CLI), on page 328
Example: Configuring the Switch as a Member of a Multicast Group, on page 363

IGMP Versions

The switch supports IGMP version 1, IGMP version 2, and IGMP version 3. These versions are interoperable on the switch. For example, if IGMP snooping is enabled and the querier's version is IGMPv2, and the switch receives an IGMPv3 report from a host, then the switch can forward the IGMPv3 report to the multicast router.

An IGMPv3 switch can receive messages from and forward messages to a device running the Source Specific Multicast (SSM) feature.

Related Topics

Changing the IGMP Version(CLI), on page 331
Restrictions for Configuring IGMP, on page 316
Restrictions for IGMP Snooping, on page 317

IGMP Version 1

IGMP version 1 (IGMPv1) primarily uses a query-response model that enables the multicast router and multilayer switch to find which multicast groups are active (have one or more hosts interested in a multicast group) on the local subnet. IGMPv1 has other processes that enable a host to join and leave a multicast group. For more information, see RFC 1112.

IGMP Version 2

IGMPv2 extends IGMP functionality by providing such features as the IGMP leave process to reduce leave latency, group-specific queries, and an explicit maximum query response time. IGMPv2 also adds the capability

for routers to elect the IGMP querier without depending on the multicast protocol to perform this task. For more information, see RFC 2236.

Note IGMP version 2 is the default version for the switch.

IGMP Version 3

The switch supports IGMP version 3.

An IGMPv3 switch supports Basic IGMPv3 Snooping Support (BISS), which includes support for the snooping features on IGMPv1 and IGMPv2 switches and for IGMPv3 membership report messages. BISS constrains the flooding of multicast traffic when your network includes IGMPv3 hosts. It constrains traffic to approximately the same set of ports as the IGMP snooping feature on IGMPv2 or IGMPv1 hosts.

An IGMPv3 switch can receive messages from and forward messages to a device running the Source Specific Multicast (SSM) feature.

IGMPv3 Host Signaling

IGMPv3 is the third version of the IETF standards track protocol in which hosts signal membership to last-hop devices of multicast groups. IGMPv3 introduces the ability for hosts to signal group membership that allows filtering capabilities with respect to sources. A host can signal either that it wants to receive traffic from all sources sending to a group except for some specific sources (a mode called EXCLUDE) or that it wants to receive traffic only from some specific sources sending to the group (a mode called INCLUDE).

IGMPv3 can operate with both ISM and SSM. In ISM, both EXCLUDE and INCLUDE mode reports are accepted by the last-hop router. In SSM, only INCLUDE mode reports are accepted by the last-hop router.

IGMP Versions Differences

There are three versions of IGMP, as defined by Request for Comments (RFC) documents of the Internet Engineering Task Force (IETF). IGMPv2 improves over IGMPv1 by adding the ability for a host to signal desire to leave a multicast group and IGMPv3 improves over IGMPv2 mainly by adding the ability to listen to multicast originating from a set of source IP addresses only.

Table 12: IGMP Versions

IGMP Version	Description
IGMPv1	Provides the basic query-response mechanism that allows the multicast device to determine which multicast groups are active and other processes that enable hosts to join and leave a multicast group. RFC 1112 defines the IGMPv1 host extensions for IP multicasting.
IGMPv2	Extends IGMP, allowing such capabilities as the IGMP leave process, group-specific queries, and an explicit maximum response time field. IGMPv2 also adds the capability for devices to elect the IGMP querier without dependence on the multicast protocol to perform this task. RFC 2236 defines IGMPv2.

Note By default, enabling a PIM on an interface enables IGMPv2 on that device. IGMPv2 was designed to be as backward compatible with IGMPv1 as possible. To accomplish this backward compatibility, RFC 2236 defined special interoperability rules. If your network contains legacy IGMPv1 hosts, you should be familiar with these operability rules. For more information about IGMPv1 and IGMPv2 interoperability, see RFC 2236, Internet Group Management Protocol, Version 2 .

Devices That Run IGMPv1

IGMPv1 devices send IGMP queries to the "all-hosts" multicast address of 224.0.0.1 to solicit multicast groups with active multicast receivers. The multicast receivers also can send IGMP reports to the device to notify it that they are interested in receiving a particular multicast stream. Hosts can send the report asynchronously or in response to the IGMP queries sent by the device. If more than one multicast receiver exists for the same multicast group, only one of these hosts sends an IGMP report message; the other hosts suppress their report messages.

In IGMPv1, there is no election of an IGMP querier. If more than one device on the segment exists, all the devices send periodic IGMP queries. IGMPv1 has no special mechanism by which the hosts can leave the group. If the hosts are no longer interested in receiving multicast packets for a particular group, they simply do not reply to the IGMP query packets sent from the device. The device continues sending query packets. If the device does not hear a response in three IGMP queries, the group times out and the device stops sending multicast packets on the segment for the group. If the host later wants to receive multicast packets after the timeout period, the host simply sends a new IGMP join to the device, and the device begins to forward the multicast packet again.

If there are multiple devices on a LAN, a designated router (DR) must be elected to avoid duplicating multicast traffic for connected hosts. PIM devices follow an election process to select a DR. The PIM device with the highest IP address becomes the DR.

The DR is responsible for the following tasks:

- Sending PIM register and PIM Join and Prune messages toward the rendezvous point (RP) to inform it about host group membership.
- Sending IGMP host-query messages.
- Sending host-query messages by default every 60 seconds in order to keep the IGMP overhead on hosts and networks very low.

Devices That Run IGMPv2

IGMPv2 improves the query messaging capabilities of IGMPv1.

The query and membership report messages in IGMPv2 are identical to the IGMPv1 messages with two exceptions:

- IGMPv2 query messages are broken into two categories: general queries (identical to IGMPv1 queries) and group-specific queries.
- IGMPv1 membership reports and IGMPv2 membership reports have different IGMP type codes.

IGMPv2 also enhances IGMP by providing support for the following capabilities:

- Querier election process--Provides the capability for IGMPv2 devices to elect the IGMP querier without having to rely on the multicast routing protocol to perform the process.
- Maximum Response Time field--A new field in query messages permits the IGMP querier to specify the maximum query-response time. This field permits the tuning of the query-response process to control response burstiness and to fine-tune leave latencies.
- Group-Specific Query messages--Permits the IGMP querier to perform the query operation on a specific group instead of all groups.
- Leave-Group messages--Provides hosts with a method of notifying devices on the network that they wish to leave the group.

Unlike IGMPv1, in which the DR and the IGMP querier are typically the same device, in IGMPv2 the two functions are decoupled. The DR and the IGMP querier are selected based on different criteria and may be different devices on the same subnet. The DR is the device with the highest IP address on the subnet, whereas the IGMP querier is the device with the lowest IP address.

Query messages are used to elect the IGMP querier as follows:

1. When IGMPv2 devices start, they each multicast a general query message to the all-systems group address of 224.0.0.1 with their interface address in the source IP address field of the message.
2. When an IGMPv2 device receives a general query message, the device compares the source IP address in the message with its own interface address. The device with the lowest IP address on the subnet is elected the IGMP querier.
3. All devices (excluding the querier) start the query timer, which is reset whenever a general query message is received from the IGMP querier. If the query timer expires, it is assumed that the IGMP querier has gone down, and the election process is performed again to elect a new IGMP querier.

By default, the timer is two times the query interval.

IGMP Join and Leave Process

IGMP Join Process

When a host wants to join a multicast group, the host sends one or more unsolicited membership reports for the multicast group it wants to join. The IGMP join process is the same for IGMPv1 and IGMPv2 hosts.

In IGMPv3, the join process for hosts proceeds as follows:

- When a hosts wants to join a group, it sends an IGMPv3 membership report to 224.0.0.22 with an empty EXCLUDE list.
- When a host wants to join a specific channel, it sends an IGMPv3 membership report to 224.0.0.22 with the address of the specific source included in the INCLUDE list.
- When a host wants to join a group excluding particular sources, it sends an IGMPv3 membership report to 224.0.0.22 excluding those sources in the EXCLUDE list.

Note If some IGMPv3 hosts on a LAN wish to exclude a source and others wish to include the source, then the device will send traffic for the source on the LAN (that is, inclusion trumps exclusion in this situation).

IGMP Leave Process

The method that hosts use to leave a group varies depending on the version of IGMP in operation.

IGMPv1 Leave Process

There is no leave-group message in IGMPv1 to notify the devices on the subnet that a host no longer wants to receive the multicast traffic from a specific group. The host simply stops processing traffic for the multicast group and ceases responding to IGMP queries with IGMP membership reports for the group. As a result, the only way IGMPv1 devices know that there are no longer any active receivers for a particular multicast group on a subnet is when the devices stop receiving membership reports. To facilitate this process, IGMPv1 devices associate a countdown timer with an IGMP group on a subnet. When a membership report is received for the group on the subnet, the timer is reset. For IGMPv1 devices, this timeout interval is typically three times the query interval (3 minutes). This timeout interval means that the device may continue to forward multicast traffic onto the subnet for up to 3 minutes after all hosts have left the multicast group.

IGMPv2 Leave Process

IGMPv2 incorporates a leave-group message that provides the means for a host to indicate that it wishes to stop receiving multicast traffic for a specific group. When an IGMPv2 host leaves a multicast group, if it was the last host to respond to a query with a membership report for that group, it sends a leave-group message to the all-devices multicast group (224.0.0.2).

IGMPv3 Leave Process

IGMPv3 enhances the leave process by introducing the capability for a host to stop receiving traffic from a particular group, source, or channel in IGMP by including or excluding sources, groups, or channels in IGMPv3 membership reports.

IGMP Snooping

Layer 2 switches can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

Note For more information on IP multicast and IGMP, see RFC 1112 and RFC 2236.

The multicast router (which could be a switch with the IP services feature set on the active switch) sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry. The switch creates one entry per VLAN in the IGMP snooping IP multicast forwarding table for each group from which it receives an IGMP join request.

The switch supports IP multicast group-based bridging, instead of MAC-addressed based groups. With multicast MAC address-based groups, if an IP address being configured translates (aliases) to a previously

configured MAC address or to any reserved multicast MAC addresses (in the range 224.0.0.xxx), the command fails. Because the switch uses IP multicast groups, there are no address aliasing issues.

The IP multicast groups learned through IGMP snooping are dynamic. However, you can statically configure multicast groups by using the **ip igmp snooping vlan** *vlan-id* **static** *ip_address* **interface** *interface-id* global configuration command. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings.

You can configure an IGMP snooping querier to support IGMP snooping in subnets without multicast interfaces because the multicast traffic does not need to be routed.

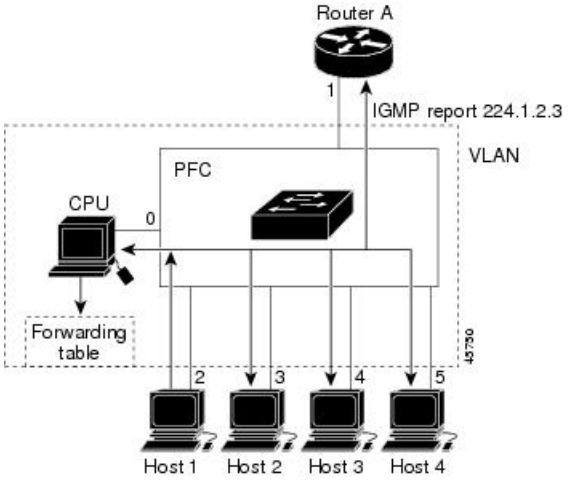
If a port spanning-tree, a port group, or a VLAN ID change occurs, the IGMP snooping-learned multicast groups from this port on the VLAN are deleted.

These sections describe IGMP snooping characteristics:

Joining a Multicast Group

Figure 25: Initial IGMP Join Message

When a host connected to the switch wants to join an IP multicast group and it is an IGMP version 2 client, it sends an unsolicited IGMP join message, specifying the IP multicast group to join. Alternatively, when the switch receives a general query from the router, it forwards the query to all ports in the VLAN. IGMP version 1 or version 2 hosts wanting to join the multicast group respond by sending a join message to the switch. The switch CPU creates a multicast forwarding-table entry for the group if it is not already present. The CPU also adds the interface where the join message was received to the forwarding-table entry. The host associated with that interface receives multicast traffic for that multicast group.



Router A sends a general query to the switch, which forwards the query to ports 2 through 5, all of which are members of the same VLAN. Host 1 wants to join multicast group 224.1.2.3 and multicasts an IGMP membership report (IGMP join message) to the group. The switch CPU uses the information in the IGMP report to set up a forwarding-table entry that includes the port numbers connected to Host 1 and to the router.

Table 13: IGMP Snooping Forwarding Table

Destination Address	Type of Packet	Ports
224.1.2.3	IGMP	1, 2

The switch hardware can distinguish IGMP information packets from other packets for the multicast group. The information in the table tells the switching engine to send frames addressed to the 224.1.2.3 multicast IP address that are not IGMP packets to the router and to the host that has joined the group.

Figure 26: Second Host Joining a Multicast Group

If another host (for example, Host 4) sends an unsolicited IGMP join message for the same group, the CPU receives that message and adds the port number of Host 4 to the forwarding table. Because the forwarding table directs IGMP messages only to the CPU, the message is not flooded to other ports on the switch. Any known multicast traffic is forwarded to the group and not to the CPU.

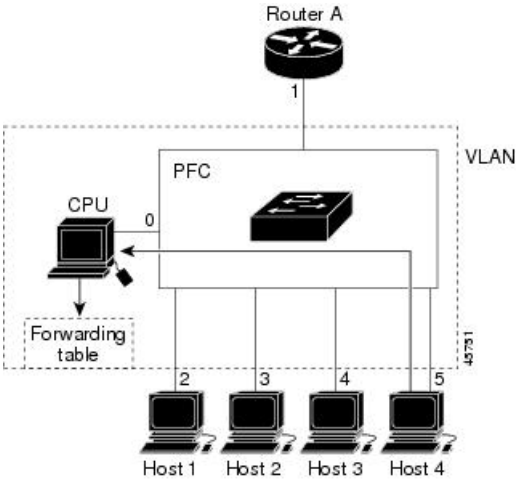


Table 14: Updated IGMP Snooping Forwarding Table

Destination Address	Type of Packet	Ports
224.1.2.3	IGMP	1, 2, 5

Related Topics

Configuring the Switch as a Member of a Group (CLI), on page 328
Example: Configuring the Switch as a Member of a Multicast Group, on page 363

Leaving a Multicast Group

The router sends periodic multicast general queries, and the switch forwards these queries through all ports in the VLAN. Interested hosts respond to the queries. If at least one host in the VLAN wants to receive multicast traffic, the router continues forwarding the multicast traffic to the VLAN. The switch forwards multicast group traffic only to those hosts listed in the forwarding table for that IP multicast group maintained by IGMP snooping.

When hosts want to leave a multicast group, they can silently leave, or they can send a leave message. When the switch receives a leave message from a host, it sends a group-specific query to learn if any other devices connected to that interface are interested in traffic for the specific multicast group. The switch then updates the forwarding table for that MAC group so that only those hosts interested in receiving multicast traffic for the group are listed in the forwarding table. If the router receives no reports from a VLAN, it removes the group for the VLAN from its IGMP cache.

Immediate Leave

The switch uses IGMP snooping Immediate Leave to remove from the forwarding table an interface that sends a leave message without the switch sending group-specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Immediate Leave ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are simultaneously in use.

Immediate Leave is only supported on IGMP version 2 hosts. IGMP version 2 is the default version for the switch.

Note You should use the Immediate Leave feature only on VLANs where a single host is connected to each port. If Immediate Leave is enabled on VLANs where more than one host is connected to a port, some hosts may be dropped inadvertently.

Related Topics

Enabling IGMP Immediate Leave (CLI), on page 349

IGMP Configurable-Leave Timer

You can configure the time that the switch waits after sending a group-specific query to determine if hosts are still interested in a specific multicast group. The IGMP leave response time can be configured from 100 to 32767 milliseconds.

Related Topics

Configuring the IGMP Leave Timer (CLI), on page 350

IGMP Report Suppression

Note IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The switch uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP report suppression is enabled (the default), the switch sends the first IGMP report from all hosts for a group to all the multicast routers. The switch does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the switch forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all the multicast routers.

If the multicast router query also includes requests for IGMPv3 reports, the switch forwards all IGMPv1, IGMPv2, and IGMPv3 reports for a group to the multicast devices.

If you disable IGMP report suppression, all IGMP reports are forwarded to the multicast routers.

Related Topics

Disabling IGMP Report Suppression (CLI), on page 359

IGMP Filtering and Throttling

In some environments, for example, metropolitan or multiple-dwelling unit (MDU) installations, you might want to control the set of multicast groups to which a user on a switch port can belong. You can control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan. You might also want to limit the number of multicast groups to which a user on a switch port can belong.

With the IGMP filtering feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing. You can also set the maximum number of IGMP groups that a Layer 2 interface can join.

IGMP filtering controls only group-specific query and membership reports, including join and leave reports. It does not control general IGMP queries. IGMP filtering has no relationship with the function that directs the forwarding of IP multicast traffic. The filtering feature operates in the same manner whether CGMP or MVR is used to forward the multicast traffic.

IGMP filtering applies only to the dynamic learning of IP multicast group addresses, not static configuration.

With the IGMP throttling feature, you can set the maximum number of IGMP groups that a Layer 2 interface can join. If the maximum number of IGMP groups is set, the IGMP snooping forwarding table contains the maximum number of entries, and the interface receives an IGMP join report, you can configure an interface to drop the IGMP report or to replace the randomly selected multicast entry with the received IGMP report.

Note IGMPv3 join and leave messages are not supported on switches running IGMP filtering.

Default IGMP Configuration

This table displays the default IGMP configuration for the switch.

Table 15: Default IGMP Configuration

Feature	Default Setting
Multilayer switch as a member of a multicast group	No group memberships are defined.
Access to multicast groups	All groups are allowed on an interface.
IGMP version	Version 2 on all interfaces.
IGMP host-query message interval	60 seconds on all interfaces.
IGMP query timeout	60 seconds on all interfaces.
IGMP maximum query response time	10 seconds on all interfaces.
Multilayer switch as a statically connected member	Disabled.

Default IGMP Snooping Configuration

This table displays the default IGMP snooping configuration for the switch.

Table 16: Default IGMP Snooping Configuration

Feature	Default Setting
IGMP snooping	Enabled globally and per VLAN
Multicast routers	None configured
IGMP snooping Immediate Leave	Disabled
Static groups	None configured
TCN[1] flood query count	2
TCN query solicitation	Disabled
IGMP snooping querier	Disabled
IGMP report suppression	Enabled

[1] (1) TCN = Topology Change Notification

Default IGMP Filtering and Throttling Configuration

This table displays the default IGMP filtering and throttling configuration for the switch.

Table 17: Default IGMP Filtering Configuration

Feature	Default Setting
IGMP filters	None applied.
IGMP maximum number of IGMP groups	No maximum set. **Note** When the maximum number of groups is in the forwarding table, the default IGMP throttling action is to deny the IGMP report.
IGMP profiles	None defined.
IGMP profile action	Deny the range addresses.

How to Configure IGMP

Configuring the Switch as a Member of a Group (CLI)

You can configure the switch as a member of a multicast group and discover multicast reachability in a network. If all the multicast-capable routers and multilayer switches that you administer are members of a multicast group, pinging that group causes all of these devices to respond. The devices respond to ICMP echo-request packets addressed to a group of which they are members. Another example is the multicast trace-route tools provided in the software.

⚠

Caution Performing this procedure might impact the CPU performance because the CPU will receive all data traffic for the group address.

This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Specifies the interface on which you want to enable multicast routing, and enters interface configuration mode.
Step 4	**ip igmp join-group** *group-address* **Example:** `Switch(config-if)# ip igmp join-group 225.2.2.2`	Configures the switch to join a multicast group. By default, no group memberships are defined. For *group-address*, specify the multicast IP address in dotted decimal notation.
Step 5	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Switch(config)# end`	
Step 6	**show ip igmp interface** [*interface-id*] **Example:** `Switch# show ip igmp interface`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Joining a Multicast Group, on page 323
Example: Configuring the Switch as a Member of a Multicast Group, on page 363
IGMP Multicast Addresses, on page 318

Controlling Access to IP Multicast Group (CLI)

The switch sends IGMP host-query messages to find which multicast groups have members on attached local networks. The switch then forwards to these group members all packets addressed to the multicast group. You can place a filter on each interface to restrict the multicast groups that hosts on the subnet serviced by the interface can join.

To limit the number of joins on the interface, configure the port for the filter which associates with the IGMP profile.

This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose

Step 3	**ip igmp profile**
	Example:
	`Switch(config)# ip igmp profile 10`
	`Switch(config-igmp-profile)# ?`
		Enters an IGMP filter profile number from 1 to 4294967295.
		For additional information about configuring IGMP filter profiles, see Configuring IGMP Profiles (CLI), on page 337.

Step 4	**permit** **Example:** `Switch(config-igmp-profile)# permit 229.9.9.0`	Enters an IGMP profile configuration action. The following IGMP profile configuration actions are supported: • **deny**—Matching IP addresses are denied. • **exit**—Exits from the IGMP profile configuration mode. • **no**—Negates a command or set its defaults. • **permit**—Matching addresses are permitted. • **range**—Adds a range to the set.
Step 5	**exit** **Example:** `Switch(config-igmp-profile)# exit`	Returns to global configuration mode.
Step 6	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Specifies the interface to be configured, and enters interface configuration mode.
Step 7	**ip igmp filter** *filter_number* **Example:** `Switch(config-if)# ip igmp filter 10`	Specifies the IGMP filter profile number. For additional information about applying IGMP filter profiles, see Applying IGMP Profiles (CLI), on page 339.
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 9	**show ip igmp interface** [*interface-id*] **Example:**	Verifies your entries.

	Command or Action	Purpose
	`Switch# show ip igmp interface`	
Step 10	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Changing the IGMP Version(CLI)

By default, the switch uses IGMP Version 2, which provides features such as the IGMP query timeout and the maximum query response time.

All systems on the subnet must support the same version. The switch does not automatically detect Version 1 systems and switch to Version 1. You can mix Version 1 and Version 2 hosts on the subnet because Version 2 routers or switches always work correctly with IGMPv1 hosts.

Configure the switch for Version 1 if your hosts do not support Version 2.

This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Specifies the interface to be configured, and enters the interface configuration mode.

	Command or Action	Purpose
Step 4	**ip igmp version** {**1** | **2** | **3** } **Example:** `Switch(config-if)# ip igmp version 2`	Specifies the IGMP version that the switch uses. **Note** If you change to Version 1, you cannot configure the **ip igmp query-interval** or the **ip igmp query-max-response-time** interface configuration commands. To return to the default setting, use the **no ip igmp version** interface configuration command.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show ip igmp interface** [*interface-id*] **Example:** `Switch# show ip igmp interface`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

IGMP Versions, on page 318
Restrictions for Configuring IGMP, on page 316
Restrictions for IGMP Snooping, on page 317

Modifying the IGMP Host-Query Message Interval (CLI)

The switch periodically sends IGMP host-query messages to discover which multicast groups are present on attached networks. These messages are sent to the all-hosts multicast group (224.0.0.1) with a time-to-live (TTL) of 1. The switch sends host-query messages to refresh its knowledge of memberships present on the network. If, after some number of queries, the software discovers that no local hosts are members of a multicast group, the software stops forwarding multicast packets to the local network from remote origins for that group and sends a prune message upstream toward the source.

The switch elects a PIM designated router (DR) for the LAN (subnet). The designated router is responsible for sending IGMP host-query messages to all hosts on the LAN. In sparse mode, the designated router also sends PIM register and PIM join messages toward the RP router. With IGMPv2, the DR is the router or multilayer switch with the highest IP address. With IGMPv1, the DR is elected according to the multicast routing protocol that runs on the LAN.

This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Specifies the interface on which you want to enable multicast routing, and enters interface configuration mode.
Step 4	**ip igmp query-interval** *seconds* **Example:** `Switch(config-if)# ip igmp query-interval 75`	Configures the frequency at which the designated router sends IGMP host-query messages. By default, the designated router sends IGMP host-query messages every 60 seconds to keep the IGMP overhead very low on hosts and networks.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show ip igmp interface** [*interface-id*] **Example:** `Switch# show ip igmp interface`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Changing the IGMP Query Timeout for IGMPv2 (CLI)

If you are using IGMPv2, you can specify the period of time before the switch takes over as the querier for the interface. By default, the switch waits twice the query interval period controlled by the **ip igmp query-interval** interface configuration command. After that time, if the switch has received no queries, it becomes the querier.

This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Specifies the interface on which you want to enable multicast routing, and enters interface configuration mode.
Step 4	**ip igmp querier-timeout** *seconds* **Example:** `Switch(config-if)# ip igmp querier-timeout 120`	Specifies the IGMP query timeout. The default is 60 seconds (twice the query interval). The range is 60 to 300.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show ip igmp interface** [*interface-id*] **Example:** `Switch# show ip igmp interface`	Verifies your entries.

	Command or Action	Purpose
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Changing the Maximum Query Response Time for IGMPv2 (CLI)

If you are using IGMPv2, you can change the maximum query response time advertised in IGMP queries. The maximum query response time enables the switch to quickly detect that there are no more directly connected group members on a LAN. Decreasing the value enables the switch to prune groups faster.

This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Specifies the interface on which you want to enable multicast routing, and enters interface configuration mode.
Step 4	**ip igmp query-max-response-time** *seconds* **Example:** `Switch(config-if)# ip igmp query-max-response-time 15`	Changes the maximum query response time advertised in IGMP queries. The default is 10 seconds. The range is 1 to 25.
Step 5	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Switch(config)# end`	
Step 6	**show ip igmp interface** [*interface-id*] **Example:** `Switch# show ip igmp interface`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring the Switch as a Statically Connected Member (CLI)

At various times, either there is not a group member on a network segment or a host that cannot report its group membership by using IGMP. However, you may want multicast traffic to be sent to that network segment. The following commands are used to pull multicast traffic down to a network segment:

- **ip igmp join-group**—The switch accepts the multicast packets in addition to forwarding them. Accepting the multicast packets prevents the switch from fast switching.
- **ip igmp static-group**—The switch does not accept the packets itself, but only forwards them. This method enables fast switching. The outgoing interface appears in the IGMP cache, but the switch itself is not a member, as evidenced by lack of an L (local) flag in the multicast route entry.

This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Specifies the interface on which you want to enable multicast routing, and enters interface configuration mode.
Step 4	**ip igmp static-group** *group-address* **Example:** `Switch(config-if)# ip igmp static-group 239.100.100.101`	Configures the switch as a statically connected member of a group. By default, this feature is disabled.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show ip igmp interface** [*interface-id*] **Example:** `Switch# show ip igmp interface gigabitethernet 1/0/1`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring IGMP Profiles (CLI)

Follow these steps to create an IGMP profile:

This task is optional.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip igmp profile** *profile number* **Example:** `Switch(config)# ip igmp profile 3`	Assigns a number to the profile you are configuring, and enters IGMP profile configuration mode. The profile number range is 1 to 4294967295. When you are in IGMP profile configuration mode, you can create the profile by using these commands: • **deny**—Specifies that matching addresses are denied; this is the default. • **exit**—Exits from igmp-profile configuration mode. • **no**—Negates a command or returns to its defaults. • **permit**—Specifies that matching addresses are permitted. • **range**—Specifies a range of IP addresses for the profile. You can enter a single IP address or a range with a start and an end address. The default is for the switch to have no IGMP profiles configured. **Note** To delete a profile, use the **no ip igmp profile** *profile number* global configuration command.
Step 4	**permit** | **deny** **Example:** `Switch(config-igmp-profile)# permit`	(Optional) Sets the action to permit or deny access to the IP multicast address. If no action is configured, the default for the profile is to deny access.
Step 5	**range** *ip multicast address* **Example:** `Switch(config-igmp-profile)# range 229.9.9.0`	Enters the IP multicast address or range of IP multicast addresses to which access is being controlled. If entering a range, enter the low IP multicast address, a space, and the high IP multicast address. You can use the **range** command multiple times to enter multiple addresses or ranges of addresses.

	Command or Action	Purpose
		Note To delete an IP multicast address or range of IP multicast addresses, use the **no range** *ip multicast address* IGMP profile configuration command.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	**show ip igmp profile** *profile number* **Example:** `Switch# show ip igmp profile 3`	Verifies the profile configuration.
Step 8	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 9	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Applying IGMP Profiles (CLI)

To control access as defined in an IGMP profile, you have to apply the profile to the appropriate interfaces. You can apply IGMP profiles only to Layer 2 access ports; you cannot apply IGMP profiles to routed ports or SVIs. You cannot apply profiles to ports that belong to an EtherChannel port group. You can apply a profile to multiple interfaces, but each interface can have only one profile applied to it.

Follow these steps to apply an IGMP profile to a switch port:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/1`	Specifies the physical interface, and enters interface configuration mode. The interface must be a Layer 2 port that does not belong to an EtherChannel port group.
Step 4	**ip igmp filter** *profile number* **Example:** `Switch(config-if)# ip igmp filter 321`	Applies the specified IGMP profile to the interface. The range is 1 to 4294967295. **Note** To remove a profile from an interface, use the **no ip igmp filter** *profile number* interface configuration command.
Step 5	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Setting the Maximum Number of IGMP Groups (CLI)

Follow these steps to set the maximum number of IGMP groups that a Layer 2 interface can join:

Before you begin

This restriction can be applied to Layer 2 ports only; you cannot set a maximum number of IGMP groups on routed ports or SVIs. You also can use this command on a logical EtherChannel interface but cannot use it on ports that belong to an EtherChannel port group.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/2`	Specifies the interface to be configured, and enters interface configuration mode. The interface can be a Layer 2 port that does not belong to an EtherChannel group or a EtherChannel interface.
Step 4	**ip igmp max-groups** *number* **Example:** `Switch(config-if)# ip igmp max-groups 20`	Sets the maximum number of IGMP groups that the interface can join. The range is 0 to 4294967294. The default is to have no maximum set. **Note** The switch supports a maximum number of 4096 Layer 2 IGMP groups and 2048 Layer 3 IGMP groups.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config interface** *interface-id* **Example:** `Switch# show running-config interface gigabitethernet1/0/1`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring the IGMP Throttling Action (CLI)

After you set the maximum number of IGMP groups that a Layer 2 interface can join, you can configure an interface to replace the existing group with the new group for which the IGMP report was received.

Follow these steps to configure the throttling action when the maximum number of entries is in the forwarding table:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Specifies the physical interface to be configured, and enters interface configuration mode. The interface can be a Layer 2 port that does not belong to an EtherChannel group or an EtherChannel interface. The interface cannot be a trunk port.
Step 4	**ip igmp max-groups action** {**deny** | **replace**} **Example:** `Switch(config-if)# ip igmp max-groups action replace`	When an interface receives an IGMP report and the maximum number of entries is in the forwarding table, specifies the action that the interface takes: • **deny**—Drops the report. If you configure this throttling action, the entries that were previously in the forwarding table are not removed but are aged out. After these entries are aged out and the maximum number of entries is in the forwarding table, the switch drops the next IGMP report received on the interface. • **replace**—Replaces the existing group with the new group for which the IGMP report was received. If you configure this throttling action, the entries that were previously in the forwarding table are removed. When the maximum number of entries is in the forwarding table, the

	Command or Action	Purpose
		switch replaces a randomly selected entry with the received IGMP report. To prevent the switch from removing the forwarding-table entries, you can configure the IGMP throttling action before an interface adds entries to the forwarding table. **Note** To return to the default action of dropping the report, use the **no ip igmp max-groups action** interface configuration command.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config interface** *interface-id* **Example:** `Switch# show running-config interface gigabitethernet1/0/1`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

How to Configure IGMP Snooping

Enabling IGMP Snooping

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**ip igmp snooping** **Example:** `Device(config)# ip igmp snooping`	Globally enables IGMP snooping after it has been disabled.
Step 4	**bridge-domain** *bridge-id* **Example:** `Device(config)# bridge-domain 100`	(Optional) Enters bridge domain configuration mode.
Step 5	**ip igmp snooping** **Example:** `Device(config-bdomain)# ip igmp snooping`	(Optional) Enables IGMP snooping on the bridge domain interface being configured. • Required only if IGMP snooping was previously explicitly disabled on the specified bridge domain.
Step 6	**end** **Example:** `Device(config-bdomain)# end`	Returns to privileged EXEC mode.

Enabling or Disabling IGMP Snooping on a VLAN Interface (CLI)

Follow these steps to enable IGMP snooping on a VLAN interface:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose
Step 3	**ip igmp snooping vlan** *vlan-id* **Example:** `Switch(config)# ip igmp snooping vlan 7`	Enables IGMP snooping on the VLAN interface. The VLAN ID range is 1 to 1001 and 1006 to 4094. IGMP snooping must be globally enabled before you can enable VLAN snooping. **Note** To disable IGMP snooping on a VLAN interface, use the **no ip igmp snooping vlan** *vlan-id* global configuration command for the specified VLAN number.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Setting the Snooping Method (CLI)

Multicast-capable router ports are added to the forwarding table for every Layer 2 multicast entry. The switch learns of the ports through one of these methods:

- Snooping on IGMP queries, Protocol-Independent Multicast (PIM) packets
- Statically connecting to a multicast router port using the **ip igmp snooping mrouter** global configuration command

Beginning in privileged EXEC mode, follow these steps to alter the method in which a VLAN interface accesses a multicast router:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip igmp snooping vlan** *vlan-id* **mrouter interface** {**GigabitEthernet** | **Port-Channel** | **TenGigabitEthernet**} **Example:** `Switch(config)# ip igmp snooping vlan 1 mrouter interface GigabitEthernet1/0/3`	Enables IGMP snooping on a VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show ip igmp snooping** **Example:** `Switch# show ip igmp snooping`	Verifies the configuration.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring a Multicast Router Port (CLI)

Perform these steps to add a multicast router port (enable a static connection to a multicast router) on the switch.

Note Static connections to multicast routers are supported only on switch ports.

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Switch> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id* **Example:** `Switch(config)# ip igmp snooping vlan 5 mrouter interface gigabitethernet1/0/1`	Specifies the multicast router VLAN ID and the interface to the multicast router. • The VLAN ID range is 1 to 1001 and 1006 to 4094. • The interface can be a physical interface or a port channel. The port-channel range is 1 to 128. **Note** To remove a multicast router port from the VLAN, use the **no ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id* global configuration command.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show ip igmp snooping mrouter** [**vlan** *vlan-id*] **Example:** `Switch# show ip igmp snooping mrouter vlan 5`	Verifies that IGMP snooping is enabled on the VLAN interface.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring a Host Statically to Join a Group (CLI)

Hosts or Layer 2 ports normally join multicast groups dynamically, but you can also statically configure a host on an interface.

Follow these steps to add a Layer 2 port as a member of a multicast group:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip igmp snooping vlan** *vlan-id* **static** *ip_address* **interface** *interface-id* **Example:** `Switch(config)# ip igmp snooping vlan 105 static 230.0.0.1 interface gigabitethernet1/0/1`	Statically configures a Layer 2 port as a member of a multicast group: • *vlan-id* is the multicast group VLAN ID. The range is 1 to 1001 and 1006 to 4094. • *ip-address* is the group IP address. • *interface-id* is the member port. It can be a physical interface or a port channel (1 to 128). **Note** To remove the Layer 2 port from the multicast group, use the **no ip igmp snooping vlan** *vlan-id* **static** *mac-address* **interface** *interface-id* global configuration command.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show ip igmp snooping groups** **Example:** `Switch# show ip igmp snooping groups`	Verifies the member port and the IP address.

	Command or Action	Purpose
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Enabling IGMP Immediate Leave (CLI)

When you enable IGMP Immediate Leave, the switch immediately removes a port when it detects an IGMP Version 2 leave message on that port. You should use the Immediate-Leave feature only when there is a single receiver present on every port in the VLAN.

Note Immediate Leave is supported only on IGMP Version 2 hosts. IGMP Version 2 is the default version for the switch.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip igmp snooping vlan** *vlan-id* **immediate-leave** **Example:** `Switch(config)# ip igmp snooping vlan 21 immediate-leave`	Enables IGMP Immediate Leave on the VLAN interface. **Note** To disable IGMP Immediate Leave on a VLAN, use the **no ip igmp snooping vlan** *vlan-id* **immediate-leave** global configuration command.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	**show ip igmp snooping vlan** *vlan-id* **Example:** `Switch# show ip igmp snooping vlan 21`	Verifies that Immediate Leave is enabled on the VLAN interface.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Related Topics

Immediate Leave , on page 325

Configuring the IGMP Leave Timer (CLI)

You can configure the leave time globally or on a per-VLAN basis. Follow these steps to enable the IGMP configurable-leave timer:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip igmp snooping last-member-query-interval** *time* **Example:** `Switch(config)# ip igmp snooping last-member-query-interval 1000`	Configures the IGMP leave timer globally. The range is 100 to 32767 milliseconds. The default leave time is 1000 milliseconds. **Note** To globally reset the IGMP leave timer to the default setting, use the **no ip igmp snooping last-member-query-interval** global configuration command.

	Command or Action	Purpose
Step 4	**ip igmp snooping vlan** *vlan-id* **last-member-query-interval** *time* **Example:** `Switch(config)# ip igmp snooping vlan 210 last-member-query-interval 1000`	(Optional) Configures the IGMP leave time on the VLAN interface. The range is 100 to 32767 milliseconds. **Note** Configuring the leave time on a VLAN overrides the globally configured timer. **Note** To remove the configured IGMP leave-time setting from the specified VLAN, use the **no ip igmp snooping vlan** *vlan-id* **last-member-query-interval** global configuration command.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show ip igmp snooping** **Example:** `Switch# show ip igmp snooping`	(Optional) Displays the configured IGMP leave time.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

IGMP Configurable-Leave Timer, on page 325

Configuring the IGMP Robustness-Variable (CLI)

Use the following procedure to configure the IGMP robustness variable on the switch.

The robustness variable is the integer used by IGMP snooping during calculations for IGMP messages. The robustness variable provides fine tuning to allow for expected packet loss.

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Switch> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip igmp snooping robustness-variable** *count* **Example:** `Switch(config)# ip igmp snooping robustness-variable 3`	Configures the IGMP robustness variable. The range is 1 to 3 times. The recommended value for the robustness variable is 2. Use this command to change the value of the robustness variable for IGMP snooping from the default (2) to a specified value.
Step 4	**ip igmp snooping vlan** *vlan-id* **robustness-variable** *count* **Example:** `Switch(config)#ip igmp snooping vlan 100 robustness-variable 3`	(Optional) Configures the IGMP robustness variable on the VLAN interface. The range is 1 to 3 times. The recommended value for the robustness variable is 2. **Note** Configuring the robustness variable count on a VLAN overrides the globally configured value.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show ip igmp snooping** **Example:** `Switch# show ip igmp snooping`	(Optional) Displays the configured IGMP robustness variable count.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring the IGMP Last Member Query Count (CLI)

To configure the number of times the switch sends IGMP group-specific or group-source-specific (with IGMP version 3) query messages in response to receiving a group-specific or group-source-specific leave message, use this command.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip igmp snooping last-member-query-count** *count* **Example:** `Switch(config)# ip igmp snooping last-member-query-count 3`	Configures the IGMP last member query count. The range is 1 to 7 messages. The default is 2 messages.
Step 4	**ip igmp snooping vlan** *vlan-id* **last-member-query-count** *count* **Example:** `Switch(config)#ip igmp snooping vlan 100 last-member-query-count 3`	(Optional) Configures the IGMP last member query count on the VLAN interface. The range is 1 to 7 messages. **Note** Configuring the last member query count on a VLAN overrides the globally configured timer.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show ip igmp snooping** **Example:** `Switch# show ip igmp snooping`	(Optional) Displays the configured IGMP last member query count.

	Command or Action	Purpose
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring TCN-Related Commands

Controlling the Multicast Flooding Time After a TCN Event (CLI)

You can configure the number of general queries by which multicast data traffic is flooded after a topology change notification (TCN) event. If you set the TCN flood query count to 1 the flooding stops after receiving 1 general query. If you set the count to 7, the flooding continues until 7 general queries are received. Groups are relearned based on the general queries received during the TCN event.

Some examples of TCN events are when the client location is changed and the receiver is on same port that was blocked but is now forwarding, and when a port goes down without sending a leave message.

Follow these steps to configure the TCN flood query count:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip igmp snooping tcn flood query count** *count* **Example:** `Switch(config)# ip igmp snooping tcn flood query count 3`	Specifies the number of IGMP general queries for which the multicast traffic is flooded. The range is 1 to 10. The default, the flooding query count is 2. **Note** To return to the default flooding query count, use the **no ip igmp snooping tcn flood query count** global configuration command.
Step 4	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Switch(config)# end`	
Step 5	**show ip igmp snooping** **Example:** `Switch# show ip igmp snooping`	Verifies the TCN settings.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Recovering from Flood Mode (CLI)

When a topology change occurs, the spanning-tree root sends a special IGMP leave message (also known as global leave) with the group multicast address 0.0.0.0. However, you can enable the switch to send the global leave message whether it is the spanning-tree root or not. When the router receives this special leave, it immediately sends general queries, which expedite the process of recovering from the flood mode during the TCN event. Leaves are always sent if the switch is the spanning-tree root regardless of this configuration.

Follow these steps to enable sending of leave messages:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip igmp snooping tcn query solicit** **Example:** `Switch(config)# ip igmp snooping tcn query solicit`	Sends an IGMP leave message (global leave) to speed the process of recovering from the flood mode caused during a TCN event. By default, query solicitation is disabled. **Note** To return to the default query solicitation, use the **no ip igmp snooping tcn query solicit** global configuration command.

	Command or Action	Purpose
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show ip igmp snooping** **Example:** `Switch# show ip igmp snooping`	Verifies the TCN settings.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Disabling Multicast Flooding During a TCN Event (CLI)

When the switch receives a TCN, multicast traffic is flooded to all the ports until 2 general queries are received. If the switch has many ports with attached hosts that are subscribed to different multicast groups, this flooding might exceed the capacity of the link and cause packet loss. Follow these steps to control TCN flooding:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Specifies the interface to be configured, and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**no ip igmp snooping tcn flood** **Example:** `Switch(config-if)# no ip igmp snooping tcn flood`	Disables the flooding of multicast traffic during a spanning-tree TCN event. By default, multicast flooding is enabled on an interface. **Note** To re-enable multicast flooding on an interface, use the **ip igmp snooping tcn flood** interface configuration command.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show ip igmp snooping** **Example:** `Switch# show ip igmp snooping`	Verifies the TCN settings.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring the IGMP Snooping Querier (CLI)

Follow these steps to enable the IGMP snooping querier feature in a VLAN:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose
Step 3	**ip igmp snooping querier** **Example:** `Switch(config)# ip igmp snooping querier`	Enables the IGMP snooping querier.
Step 4	**ip igmp snooping querier address** *ip_address* **Example:** `Switch(config)# ip igmp snooping querier address 172.16.24.1`	(Optional) Specifies an IP address for the IGMP snooping querier. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier. **Note** The IGMP snooping querier does not generate an IGMP general query if it cannot find an IP address on the switch.
Step 5	**ip igmp snooping querier query-interval** *interval-count* **Example:** `Switch(config)# ip igmp snooping querier query-interval 30`	(Optional) Sets the interval between IGMP queriers. The range is 1 to 18000 seconds.
Step 6	**ip igmp snooping querier tcn query** [**count** *count* | **interval** *interval*] **Example:** `Switch(config)# ip igmp snooping querier tcn query interval 20`	(Optional) Sets the time between Topology Change Notification (TCN) queries. The count range is 1 to 10. The interval range is 1 to 255 seconds.
Step 7	**ip igmp snooping querier timer expiry** *timeout* **Example:** `Switch(config)# ip igmp snooping querier timer expiry 180`	(Optional) Sets the length of time until the IGMP querier expires. The range is 60 to 300 seconds.
Step 8	**ip igmp snooping querier version** *version* **Example:** `Switch(config)# ip igmp snooping querier version 2`	(Optional) Selects the IGMP version number that the querier feature uses. Select 1 or 2.
Step 9	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Switch(config)# end`	
Step 10	**show ip igmp snooping vlan** *vlan-id* **Example:** `Switch# show ip igmp snooping vlan 30`	(Optional) Verifies that the IGMP snooping querier is enabled on the VLAN interface. The VLAN ID range is 1 to 1001 and 1006 to 4094.
Step 11	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Disabling IGMP Report Suppression (CLI)

Follow these steps to disable IGMP report suppression:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**no ip igmp snooping report-suppression** **Example:** `Switch(config)# no ip igmp snooping report-suppression`	Disables IGMP report suppression. When report suppression is disabled, all IGMP reports are forwarded to the multicast routers. IGMP report suppression is enabled by default. When IGMP report supression is enabled, the switch forwards only one IGMP report per multicast router query. **Note** To re-enable IGMP report suppression, use the **ip igmp snooping report-suppression** global configuration command.

	Command or Action	Purpose
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show ip igmp snooping** **Example:** `Switch# show ip igmp snooping`	Verifies that IGMP report suppression is disabled.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

IGMP Report Suppression, on page 325

Monitoring IGMP

You can display specific statistics, such as the contents of IP routing tables, caches, and databases.

Note This release does not support per-route statistics.

You can display information to learn resource usage and solve network problems. You can also display information about node reachability and discover the routing path that packets of your device are taking through the network.

You can use any of the privileged EXEC commands in the following table to display various routing statistics.

Table 18: Commands for Displaying System and Network Statistics

Command	Purpose
ping [*group-name* | *group-address*]	Sends an ICMP Echo Request to a multicast group address.
show ip igmp filter	Displays IGMP filter information.
show ip igmp groups [*type-number* | *detail*]	Displays the multicast groups that are directly connected to the switch and that were learned through IGMP.

Command	Purpose
show ip igmp interface [*type number*]	Displays multicast-related information about an interface.
show ip igmp membership [*name/group address* | **all** | **tracked**]	Displays IGMP membership information for forwarding.
show ip igmp profile [*profile_number*]	Displays IGMP profile information.
show ip igmp ssm-mapping [*hostname/IP address*]	Displays IGMP SSM mapping information.
show ip igmp static-group {**class-map** [**interface** [*type*]]	Displays static group information.
show ip igmp vrf	Displays the selected VPN routing/forwarding instance by name.

Monitoring IGMP Snooping Information

You can display IGMP snooping information for dynamically learned and statically configured router ports and VLAN interfaces. You can also display MAC address multicast entries for a VLAN configured for IGMP snooping.

Table 19: Commands for Displaying IGMP Snooping Information

Command	Purpose
show ip igmp snooping detail	Displays the operational state information.
show ip igmp snooping groups [**count** | [**vlan** *vlan-id* [*A.B.C.D* | **count**]]	Displays multicast table information for the switch or about a specific parameter: • **count**—Displays the total number of groups. • **vlan**—Displays group information by VLAN ID.
show ip igmp snooping igmpv2-tracking	Displays the IGMP snooping tracking. **Note** This command displays group and IP address entries only for wireless multicast IGMP joins and not for wired IGMP joins. Wireless IP multicast must be enabled for this command to display.

Command	Purpose
show ip igmp snooping mrouter [**vlan** *vlan-id*]	Displays information on dynamically learned and manually configured multicast router interfaces. **Note** When you enable IGMP snooping, the switch automatically learns the interface to which a multicast router is connected. These are dynamically learned interfaces. (Optional) Enter **vlan** *vlan-id* to display information for a single VLAN.
show ip igmp snooping querier [**detail** | **vlan** *vlan-id*]	Displays information about the IP address and receiving port for the most-recently received IGMP query messages in the VLAN. (Optional) Enter **detail** to display the detailed IGMP querier information in a VLAN. (Optional) Enter **vlan** *vlan-id* to display information for a single VLAN.
show ip igmp snooping [**vlan** *vlan-id* [**detail**]]	Displays the snooping configuration information for all VLANs on the switch or for a specified VLAN. (Optional) Enter **vlan** *vlan-id* to display information for a single VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
show ip igmp snooping wireless mgid	Displays wireless-related events.

Monitoring IGMP Filtering and Throttling Configuration

You can display IGMP profile characteristics, and you can display the IGMP profile and maximum group configuration for all interfaces on the switch or for a specified interface. You can also display the IGMP throttling configuration for all interfaces on the switch or for a specified interface.

Table 20: Commands for Displaying IGMP Filtering and Throttling Configuration

Command	Purpose
show ip igmp profile [*profile number*]	Displays the specified IGMP profile or all the IGMP profiles defined on the switch.
show running-config [**interface** *interface-id*]	Displays the configuration of the specified interface or the configuration of all interfaces on the switch, including (if configured) the maximum number of IGMP groups to which an interface can belong and the IGMP profile applied to the interface.

Configuration Examples for IGMP

Example: Configuring the Switch as a Member of a Multicast Group

This example shows how to enable the switch to join multicast group 255.2.2.2:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip igmp join-group 255.2.2.2
Switch(config-if)#
```

Related Topics

Configuring the Switch as a Member of a Group (CLI), on page 328
Joining a Multicast Group, on page 323
IGMP Multicast Addresses, on page 318

Example: Controlling Access to Multicast Groups

To limit the number of joins on the interface, configure the port for filter which associates with the IGMP profile.

```
Switch# configure terminal
Switch(config)# ip igmp profile 10
Switch(config-igmp-profile)# ?

IGMP profile configuration commands:
deny matching addresses are denied
exit Exit from igmp profile configuration mode
no Negate a command or set its defaults
permit matching addresses are permitted
range add a range to the set

Switch(config-igmp-profile)# range 172.16.5.1
Switch(config-igmp-profile)# exit
Switch(config)#
Switch(config)# interface gigabitEthernet 2/0/10
Switch(config-if)# ip igmp filter 10
```

Examples: Configuring IGMP Snooping

This example shows how to enable a static connection to a multicast router:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 mrouter interface gigabitethernet1/0/2
Switch(config)# end
```

This example shows how to statically configure a host on a port:

```
Switch# configure terminal
```

```
Switch(config)# ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet1/0/1
Switch(config)# end
```

This example shows how to enable IGMP Immediate Leave on VLAN 130:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 130 immediate-leave
Switch(config)# end
```

This example shows how to set the IGMP snooping querier source address to 10.0.0.64:

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier 10.0.0.64
Switch(config)# end
```

This example shows how to set the IGMP snooping querier maximum response time to 25 seconds:

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier query-interval 25
Switch(config)# end
```

This example shows how to set the IGMP snooping querier timeout to 60 seconds:

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier timer expiry 60
Switch(config)# end
```

This example shows how to set the IGMP snooping querier feature to Version 2:

```
Switch# configure terminal
Switch(config)# no ip igmp snooping querier version 2
Switch(config)# end
```

Example: Configuring IGMP Profiles

This example shows how to create IGMP profile 4 allowing access to the single IP multicast address and how to verify the configuration. If the action was to deny (the default), it would not appear in the **show ip igmp profile** output display.

```
Switch(config)# ip igmp profile 4
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 229.9.9.0
Switch(config-igmp-profile)# end
Switch# show ip igmp profile 4
IGMP Profile 4
    permit
    range 229.9.9.0 229.9.9.0
```

Example: Applying IGMP Profile

This example shows how to apply IGMP profile 4 to a port:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip igmp filter 4
Switch(config-if)# end
```

Example: Setting the Maximum Number of IGMP Groups

This example shows how to limit to 25 the number of IGMP groups that a port can join:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)# end
```

Example: Interface Configuration as a Routed Port

This example shows how to configure an interface on the switch as a routed port. This configuration is required on the interface for several IP multicast routing configuration procedures that require running the **no switchport** command.

```
Switch configure terminal
Switch(config)#  interface GigabitEthernet1/0/9
Switch(config-if)# description interface to be use as routed port
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.20.20.1 255.255.255.0
Switch(config-if)# ip pim sparse-mode
Switch(config-if)# ip igmp join-group 224.1.2.3 source 15.15.15.2
Switch(config-if)# end
Switch# configure terminal
Switch# show run interface gigabitEthernet 1/0/9

Current configuration : 166 bytes
!
interface GigabitEthernet1/0/9
 no switchport
 ip address 10.20.20.1 255.255.255.0
 ip pim sparse-mode
 ip igmp static-group 224.1.2.3 source 15.15.15.2
end
```

Example: Interface Configuration as an SVI

This example shows how to configure an interface on the switch as an SVI. This configuration is required on the interface for several IP multicast routing configuration procedures that require running the **no switchport** command.

```
Switch(config)# interface vlan 150
Switch(config-if)# ip address 10.20.20.1 255.255.255.0
Switch(config-if)# ip pim sparse-mode
Switch(config-if)# ip igmp join-group 224.1.2.3 source 15.15.15.2
Switch(config-if)# end
```

```
Switch# configure terminal
Switch(config)#  ip igmp snooping vlan 20 static 224.1.2.3
interface gigabitEthernet 1/0/9
Switch# show run interface vlan 150

Current configuration : 137 bytes
!
interface Vlan150
 ip address 10.20.20.1 255.255.255.0
 ip pim sparse-mode
 ip igmp static-group 224.1.2.3 source 15.15.15.2
end
```

Additional References

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	*IP Multicast Routing Command Reference (Catalyst 3850 Switches)Cisco 5760 Multicast Command Reference (Cisco WLC 5700 Series)*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS IP SLAs commands	Cisco IOS IP Multicast Command Reference

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
RFC 1112	Host Extensions for IP Multicasting
RFC 2236	Internet Group Management Protocol, Version 2
RFC 3376	*Internet Group Management Protocol, Version 3*

MIBs

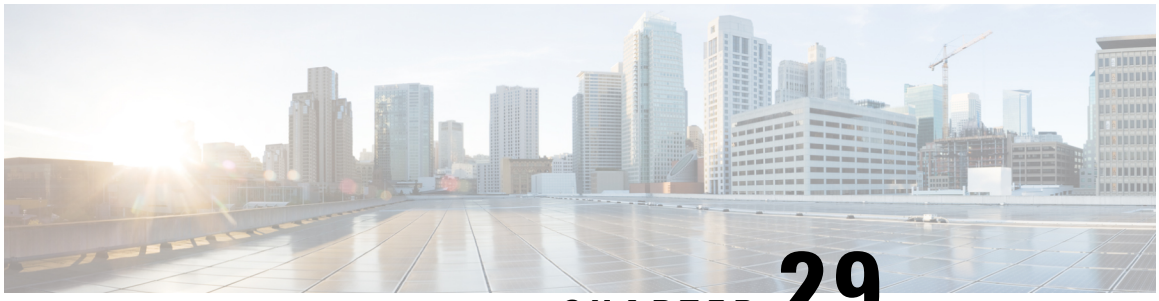
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for IGMP

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 29

Configuring Wireless Multicast

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Wireless Multicast

- The IP multicast routing must be enabled. The default routes should be available in the device. After performing these tasks, the device can then forward multicast packets and can populate its multicast routing table.
- To participate in IP multicasting, the multicast hosts, routers, and multilayer switches must have IGMP operating.
- When enabling multicast mode on the switch, a CAPWAP multicast group address should also be configured. Access points listen to the CAPWAP multicast group using IGMP.

Restrictions for Configuring Wireless Multicast

The following are the restrictions for configuring IP multicast routing:

- Access points in monitor mode, sniffer mode, or rogue detector mode do not join the CAPWAP multicast group address.
- The CAPWAP multicast group configured on the switch should be different for different switches.
- Multicast routing should not be enabled for the management interface.

Restrictions for IPv6 Snooping

The IPv6 snooping feature is not supported on Etherchannel ports.

Restrictions for IPv6 RA Guard

- The IPv6 RA Guard feature does not offer protection in environments where IPv6 traffic is tunneled.
- This feature is supported only in hardware when the ternary content addressable memory (TCAM) is programmed.
- This feature can be configured on a switch port interface in the ingress direction.
- This feature supports host mode and router mode.
- This feature is supported only in the ingress direction; it is not supported in the egress direction.
- This feature is not supported on EtherChannel and EtherChannel port members.
- This feature is not supported on trunk ports with merge mode.
- This feature is supported on auxiliary VLANs and private VLANs (PVLANs). In the case of PVLANs, primary VLAN features are inherited and merged with port features.
- Packets dropped by the IPv6 RA Guard feature can be spanned.
- If the **platform ipv6 acl icmp optimize neighbor-discovery command** is configured, the IPv6 RA Guard feature cannot be configured and an error message will be displayed. This command adds default global Internet Control Message Protocol (ICMP) entries that will override the RA guard ICMP entries.

Information About Wireless Multicast

If the network supports packet multicasting, the multicast method that the switch uses can be configured. The switch performs multicasting in two modes:

- Unicast mode—The switch unicasts every multicast packet to every access point associated to the switch. This mode is inefficient but might be required on networks that do not support multicasting.
- Multicast mode—The switch sends multicast packets to a CAPWAP multicast group. This method reduces overhead on the switch processor and shifts the work of packet replication to the network, which is much more efficient than the unicast method.

When the multicast mode is enabled and the switch receives a multicast packet from the wired LAN, the switch encapsulates the packet using CAPWAP and forwards the packet to the CAPWAP multicast group address. The switch always uses the management VLAN for sending multicast packets. Access points in the

multicast group receive the packet and forward it to all the BSSIDs mapped to the VLAN on which clients receive multicast traffic.

The switch supports all the capabilities of IGMP v1 including Multicast Listener Discovery (MLD) v1 snooping but the IGMP v2 and IGMP v3 capabilities are limited. This feature keeps track of and delivers IPv6 multicast flows to the clients that request them. To support IPv6 multicast, global multicast mode should be enabled.

Internet Group Management Protocol (IGMP) snooping is introduced to better direct multicast packets. When this feature is enabled, the switch snooping gathers IGMP reports from the clients, processes them, creates unique multicast group IDs (MGIDs) based on the Layer 3 multicast address and the VLAN number, and sends the IGMP reports to the IGMP querier. The switch then updates the access point MGID table on the access point with the client MAC address. When the switch receives multicast traffic for a particular multicast group, it forwards it to all the access points, but only those access points that have active clients listening or subscribed to that multicast group send multicast traffic on that particular WLAN. IP packets are forwarded with an MGID that is unique for an ingress VLAN and the destination multicast group. Layer 2 multicast packets are forwarded with an MGID that is unique for the ingress VLAN.

MGID is a 14-bit value filled in the 16-bit reserved field of wireless information in CAPWAP header. The remaining 2 bits should be set to zero.

Related Topics

Configuring Wireless Multicast-MCMC Mode (CLI), on page 374
Configuring Wireless Multicast-MCUC Mode (CLI), on page 375

Information About Multicast Optimization

Multicast used to be based on the group of the multicast addresses and the VLAN as one entity, MGID. With the VLAN group, duplicate packets might increase. Using the VLAN group feature, every client listens to the multicast stream on a different VLAN. As a result, the switch creates different MGIDs for each multicast address and VLAN. Therefore, in a worst case situation, the upstream router sends one copy for each VLAN, which results in as many copies as the number of VLANs in the group. Because the WLAN remains the same for all clients, multiple copies of the multicast packet are sent over the wireless network. To suppress the duplication of a multicast stream on the wireless medium between the switch and the access points, the multicast optimization feature can be used.

Multicast optimization enables you to create a multicast VLAN that can be used for multicast traffic. One of the VLANs in the switch can be configured as a multicast VLAN where multicast groups are registered. The clients are allowed to listen to a multicast stream on the multicast VLAN. The MGID is generated using the mulicast VLAN and multicast IP addresses. If multiple clients on different VLANs of the same WLAN are listening to a single multicast IP address, a single MGID is generated. The switch makes sure that all multicast streams from the clients on this VLAN group always go out on the multicast VLAN to ensure that the upstream router has one entry for all the VLANs of the VLAN group. Only one multicast stream hits the VLAN group even if the clients are on different VLANs. Therefore, the multicast packets that are sent out over the network is just one stream.

Related Topics

Configuring IP Multicast VLAN for WLAN (CLI), on page 380

IPv6 Global Policies

IPv6 global policies provide storage and access policy database services. IPv6 ND inspection and IPv6 RA guard are IPv6 global policies features. Every time an ND inspection or RA guard is configured globally, the

policy attributes are stored in the software policy database. The policy is then applied to an interface, and the software policy database entry is updated to include this interface to which the policy is applied.

IPv6 RA Guard

The IPv6 RA Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue RA guard messages that arrive at the network device platform. RAs are used by devices to announce themselves on the link. The IPv6 RA Guard feature analyzes these RAs and filters out RAs that are sent by unauthorized devices. In host mode, all RA and router redirect messages are disallowed on the port. The RA guard feature compares configuration information on the Layer 2 (L2) device with the information found in the received RA frame. Once the L2 device has validated the content of the RA frame and router redirect frame against the configuration, it forwards the RA to its unicast or multicast destination. If the RA frame content is not validated, the RA is dropped.

Information About IPv6 Snooping

IPv6 Neighbor Discovery Inspection

The IPv6 Neighbor Discovery Inspection, or IPv6 "snooping," feature bundles several Layer 2 IPv6 first-hop security features, including IPv6 Address Glean and IPv6 Device Tracking. IPv6 neighbor discovery (ND) inspection operates at Layer 2, or between Layer 2 and Layer 3, and provides IPv6 features with security and scalability. This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism, such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables and analyzes ND messages in order to build a trusted binding table. IPv6 ND messages that do not have valid bindings are dropped. An ND message is considered trustworthy if its IPv6-to-MAC mapping is verifiable.

When IPv6 ND inspection is configured on a target (which varies depending on platform target support and may include device ports, switch ports, Layer 2 interfaces, Layer 3 interfaces, and VLANs), capture instructions are downloaded to the hardware to redirect the ND protocol and Dynamic Host Configuration Protocol (DHCP) for IPv6 traffic up to the switch integrated security features (SISF) infrastructure in the routing device. For ND traffic, messages such as NS, NA, RS, RA, and REDIRECT are directed to SISF. For DHCP, UDP messages sourced from port 546 or 547 are redirected.

IPv6 ND inspection registers its "capture rules" to the classifier, which aggregates all rules from all features on a given target and installs the corresponding ACL down into the platform-dependent modules. Upon receiving redirected traffic, the classifier calls all entry points from any registered feature (for the target on which the traffic is being received), including the IPv6 ND inspection entry point. This entry point is the last to be called, so any decision (such as drop) made by another feature supersedes the IPv6 ND inspection decision.

IPv6 ND Inspection

IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables. IPv6 ND inspection analyzes neighbor discovery messages in order to build a trusted binding table database, and IPv6 neighbor discovery messages that do not have valid bindings are dropped. A neighbor discovery message is considered trustworthy if its IPv6-to-MAC mapping is verifiable.

This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism, such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

IPv6 Device Tracking

IPv6 device tracking provides IPv6 host liveness tracking so that a neighbor table can be immediately updated when an IPv6 host disappears.

IPv6 First-Hop Security Binding Table

The IPv6 First-Hop Security Binding Table recovery mechanism feature enables the binding table to recover in the event of a device reboot. A database table of IPv6 neighbors connected to the device is created from information sources such as ND snooping. This database, or binding, table is used by various IPv6 guard features to validate the link-layer address (LLA), the IPv4 or IPv6 address, and prefix binding of the neighbors to prevent spoofing and redirect attacks.

This mechanism enables the binding table to recover in the event of a device reboot. The recovery mechanism will block any data traffic sourced from an unknown source; that is, a source not already specified in the binding table and previously learned through ND or DHCP gleaning. This feature recovers the missing binding table entries when the resolution for a destination address fails in the destination guard. When a failure occurs, a binding table entry is recovered by querying the DHCP server or the destination host, depending on the configuration.

Recovery Protocols and Prefix Lists

The IPv6 First-Hop Security Binding Table Recovery Mechanism feature introduces the capability to provide a prefix list that is matched before the recovery is attempted for both DHCP and NDP.

If an address does not match the prefix list associated with the protocol, then the recovery of the binding table entry will not be attempted with that protocol. The prefix list should correspond to the prefixes that are valid for address assignment in the Layer 2 domain using the protocol. The default is that there is no prefix list, in which case the recovery is attempted for all addresses. The command to associate a prefix list to a protocol is **protocol** {**dhcp** | **ndp**} [**prefix-list** *prefix-list-name*].

IPv6 Device Tracking

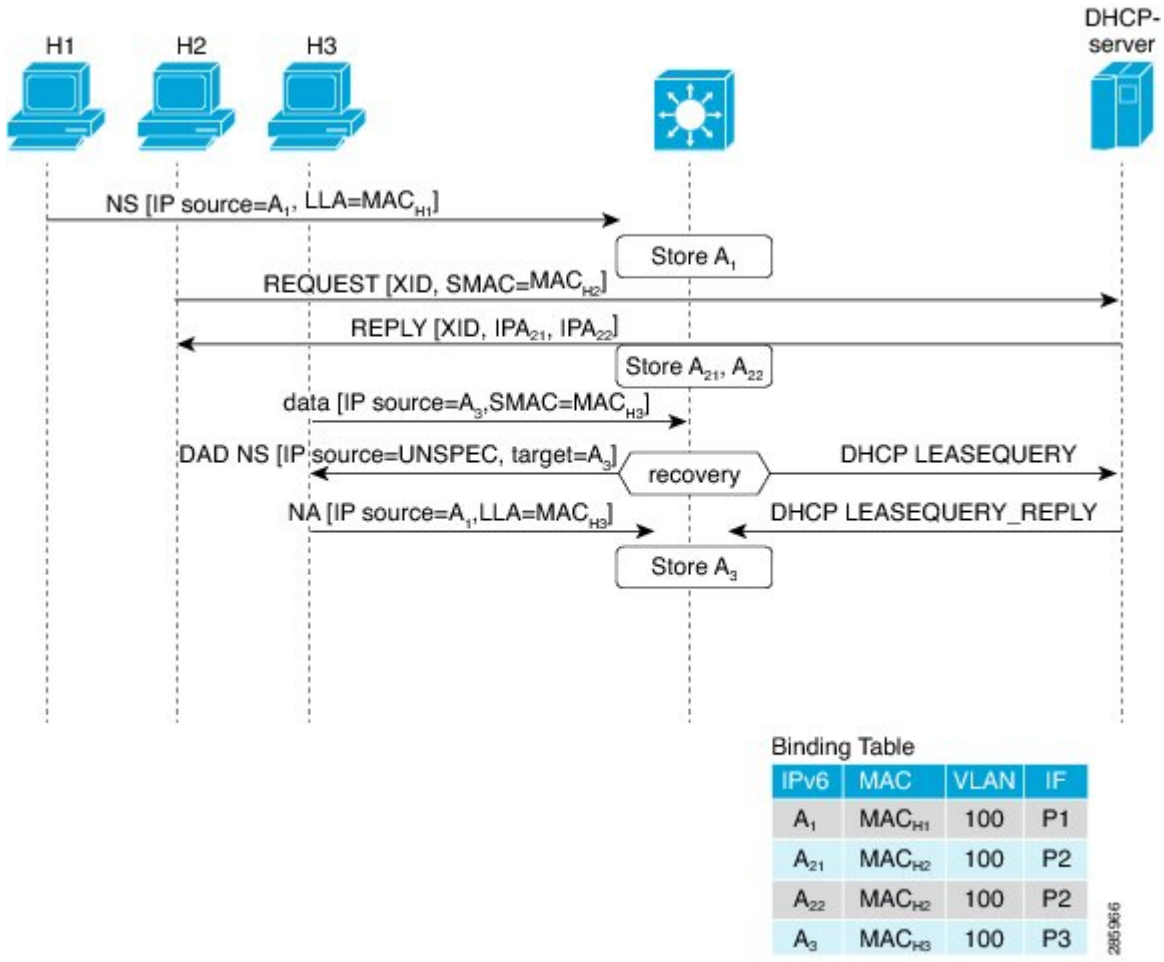
IPv6 device tracking provides IPv6 host liveness tracking so that a neighbor table can be immediately updated when an IPv6 host disappears.

IPv6 Address Glean

IPv6 address glean is the foundation for many other IPv6 features that depend on an accurate binding table. It inspects ND and DHCP messages on a link to glean addresses, and then populates the binding table with these addresses. This feature also enforces address ownership and limits the number of addresses any given node is allowed to claim.

The following figure shows how IPv6 address glean works.

Figure 27: IPv6 Address Glean



How to Configure Wireless Multicast

Configuring Wireless Multicast-MCMC Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.

Step 3	**wireless multicast**
	Example:
	`Switch(config)# wireless multicast`
	`Switch(config)# no wireless multicast`
		Enables the multicast traffic for wireless clients. The default value is disable. Add **no** in the command to disable the multicast traffic for wireless clients.

Step 4	**end** **Example:** `Switch(config)# end`	Exits the configuration mode. Alternatively, press **Ctrl-Z** to exit the configuration mode.

Related Topics

Information About Wireless Multicast, on page 370

Configuring Wireless Multicast-MCUC Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 3	**wireless multicast** **Example:** `Switch(config)# wireless multicast`	Enables the multicast traffic for wireless clients and enables mDNS bridging. The default value is disable. Add **no** in the command to disable the multicast traffic for wireless clients and disable mDNS bridging.
Step 4	**end** **Example:** `Switch(config)# end`	Exits the configuration mode. Alternatively, press **Ctrl-Z** to exit the configuration mode.

Related Topics

Information About Wireless Multicast, on page 370

Configuring IPv6 Snooping (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 3	**ipv6 mld snooping** **Example:** `Switch(config)# ipv6 mld snooping`	Enables MLD snooping.

Configuring IPv6 Snooping Policy (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 3	**ipv6 snooping policy** *policy-name* **Example:** `Switch(config)# ipv6 snooping policy mypolicy`	Configures an IPv6 snooping policy with a name.
Step 4	**security-level guard** **Example:** `Switch(config-ipv6-snooping)# security-level guard`	Configures security level to inspect and drop any unauthorized messages.

	Command or Action	Purpose
Step 5	**device-role node** **Example:** `Switch(config-ipv6-snooping)# device-role node`	Configures the role of the device, which is a node, to the attached port.
Step 6	**protocol** {**dhcp** | **ndp**} **Example:** `Switch(config-ipv6-snooping)# protocol ndp`	Sets the protocol to glean addresses in DHCP or NDP packets.

Configuring Layer 2 Port as Multicast Router Port (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 3	**ipv6 mld snooping vlan** *vlan-id* **mrouter interface Port-channel** *port-channel-interface-number* **Example:** `Switch(config)# ipv6 mld snooping vlan 2 mrouter interface Port-channel 22`	Configures a Layer 2 port as a Multicast router port. The VLAN is the client VLAN.

Configuring IPv6 RA Guard (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 3	**ipv6 nd raguard policy** *policy-name* **Example:** `Switch(config)# ipv6 nd raguard policy myraguardpolicy`	Configures a policy for RA Guard.
Step 4	**trusted-port** **Example:** `Switch(config-nd-raguard)# trusted-port`	Sets up a trusted port.
Step 5	**device-role** {**host** | **monitor** | **router** | **switch**} **Example:** `Switch(config-nd-raguard)# device-role router`	Sets the role of the device attached to the port.

Configuring Non-IP Wireless Multicast (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.

Step 3	**wireless multicast non-ip**
	Example:
	`Switch(config)# wireless multicast non-ip`
	`Switch(config)# no wireless multicast non-ip`
		Enables non-IP multicast in all VLANs. Default value is **enable**. Wireless multicast must be enabled for the traffic to pass. Add **no** in the command to disable the non-IP multicast in all VLANs.

Step 4	**wireless multicast non-ip vlan** *vlanid* **Example:** `Switch(config)# wireless multicast non-ip vlan 5`	Enables non-IP multicast per VLAN. Default value is **enable**. Both wireless multicast and wireless multicast non-IP must be enabled for traffic to pass. Add **no** in the command to disable the non-IP multicast per VLAN.

	Command or Action	Purpose
	`Switch(config)# no wireless multicast non-ip vlan 5`	
Step 5	**end** **Example:** `Switch(config)# end`	Exits the configuration mode. Alternatively, press **Ctrl-Z** to exit the configuration mode.

Configuring Wireless Broadcast (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.

Step 3	**wireless broadcast**
	Example:
	`Switch(config)# wireless broadcast`
	`Switch(config)# no wireless broadcast`
		Enables broadcast packets for wireless clients. Default value is disable. Enabling **wireless broadcast** enables broadcast traffic for each VLAN. Add **no** in the command to disable broadcasting packets.

Step 4	**wireless broadcast vlan** *vlanid*
	Example:
	`Switch(config)# wireless broadcast vlan 3`
	`Switch(config)# no wireless broadcast vlan 3`
		Enables broadcast packets for single VLAN. Default value is **enable**. Wireless broadcast must be enabled for broadcasting. Add **no** in the command to disable the broadcast traffic for each VLAN.

Step 5	**end** **Example:** `Switch(config)# end`	Exits the configuration mode. Alternatively, press **Ctrl-Z** to exit the configuration mode.

Configuring IP Multicast VLAN for WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 3	**wlan** *wlan_name* **Example:** `Switch(config)# wlan test 1`	Enters the configuration mode to configure various parameters in the WLAN.
Step 4	**shutdown** **Example:** `Switch(config-wlan)# shutdown`	Disables WLAN.

Step 5	**ip multicast vlan** {*vlan_name vlan_id*}
	Example:
	`Switch(config-wlan)# ip multicast vlan 5`
	`Switch(config-wlan)# no ip multicast vlan 5`
		Configures multicast VLAN for WLAN. Add **no** in the command to disable the multicast VLAN for WLAN.

Step 6	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Enables the disabled WLAN.
Step 7	**end** **Example:** `Switch(config)# end`	Exits the configuration mode. Alternatively, press **Ctrl-Z** to exit the configuration mode.

Related Topics

Information About Multicast Optimization, on page 371

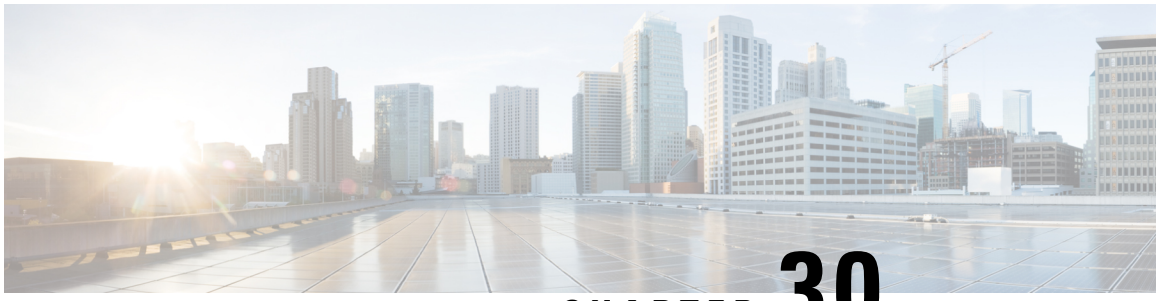
Monitoring Wireless Multicast

Table 21: Commands for Monitoring Wireless Multicast

Commands	Description
show wireless multicast	Displays the multicast status and IP multicast mode, each VLAN's broadcast and non-IP multicast status. Also displays the mDNS bridging state.
show wireless multicast group summary	Displays all (Source, Group and VLAN) lists and the corresponding MGID value.
show wireless multicast [**source** *source*] **group** *group* **vlan** *vlanid*	Displays details of the given (S,G,V) and shows all of the clients associated with it and their MC2UC status .
show ip igmp snooping wireless mcast-spi-count	Displays statistics of the number of multicast SPIs per MGID sent between IOS and the Wireless Controller Module. Displays statistics of the number of multicast SPIs per MGID sent internally between IOS and the Wireless Controller Module.
show ip igmp snooping wireless mgid	Displays the MGID mappings.
show ip igmp snooping igmpv2-tracking	Displays the client-to-SGV mappings and SGV-to-client mappings.
show ip igmp snooping querier vlan *vlanid*	Displays IGMP querier information for the specified VLAN.
show ip igmp snooping querier detail	Displays detailed IGMP querier information of all the VLANs.
show ipv6 mld snooping querier vlan *vlanid*	Displays MLD querier information for the specified VLAN.
show ipv6 mld snooping wireless mgid	Displays MGIDs for IPv6 multicast group.

Where to Go Next for Wireless Multicast

You can configure the following:



CHAPTER 30

Configuring the Service Discovery Gateway

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring the Service Discovery Gateway

The following are restrictions for configuring the Service Discovery Gateway:

- The Service Discovery Gateway does not support topologies with multiple hops. All network segments must be connected directly to it. The Service Discovery Gateway can learn services from all connected segments to build its cache and respond to requests acting as a proxy.
- The use of third-party mDNS servers or applications are not supported with this feature.
- On a Cat4500sup8e MC (3.7) running mDNS, iphone and ipads running iOS7.0 might have problems in accessing print services through mDNS.

Information about the Service Discovery Gateway and mDNS

mDNS

mDNS was defined to achieve zero configuration, with zero configuration being defined as providing the following features:

- Addressing—Allocating IP addresses to hosts
- Naming—Using names to refer to hosts instead of IP addresses
- Service discovery—Finding services automatically on the network

With mDNS, network users no longer have to assign IP addresses, assign host names, or type in names to access services on the network. Users only need to ask to see what network services are available, and choose from a list.

With mDNS, *addressing* is accomplished through the use of DHCP/DHCPv6 or IPv4 and IPv6 Link Local scoped addresses. The benefit of zero-configuration occurs when no infrastructure services such as DHCP or DNS are present and self-assigned link-local addressing can be used. The client can then select a random IPv4 address in the link-local range (169.254.0.0/24) or use its IPv6 link-local address (FE80::/10) for communication.

With mDNS, *naming* (name-to-address translation on a local network using mDNS) queries are sent over the local network using link-local scoped IP multicast. Because these DNS queries are sent to a multicast address (IPv4 address 224.0.0.251 or IPv6 address FF02::FB), no single DNS server with global knowledge is required to answer the queries. When a service or device sees a query for any service it is aware of, it provides a DNS response with the information from its cache.

With mDNS, *service discovery* is accomplished by browsing. An mDNS query is sent out for a given service type and domain, and any device that is aware of matching services replies with service information. The result is a list of available services for the user to choose from.

The mDNS protocol (mDNS-RFC), together with DNS Service Discovery (DNS-SD-RFC) achieves the zero-configuration addressing, naming, and service discovery.

mDNS-SD

Multicast DNS Service Discovery (mDNS-SD) uses DNS protocol semantics and multicast over well-known multicast addresses to achieve zero configuration service discovery. DNS packets are sent to and received on port 5353 using a multicast address of 224.0.0.251 and its IPv6 equivalent FF02::FB.

Because mDNS uses a link-local multicast address, its scope is limited to a single physical or logical LAN. If the networking reach needs to be extended to a distributed campus or to a wide-area environment consisting of many different networking technologies, mDNS gateway is implemented. An mDNS gateway provides a transport for mDNS packets across Layer 3 boundaries by filtering, caching, and redistributing services from one Layer 3 domain to another.

mDNS-SD Considerations for Wireless Clients

- mDNS packets can be sent out of Layer 3 interfaces that might not have an IP address.
- Packets with mDNS multicast IP and multicast MAC are sent on a multicast CAPWAP tunnel, if multicast-multicast mode is enabled. A multicast CAPWAP tunnel is a special CAPWAP tunnel used

for reducing the number of copies of multicast packet that are required to be generated for each AP CAPWAP tunnel. Sending packets on the multicast CAPWAP tunnel requires the outer IP header to be destined to the multicast CAPWAP tunnel's address, which all APs are subscribed to.

- All mDNS packet handling is done at a foreign switch for roamed clients. A foreign switch is the new switch that a roamed wireless client is actually attached to, which is called the point of attachment.

Service Discovery Gateway

The Service Discovery Gateway feature enables multicast Domain Name System (mDNS) to operate across Layer 3 boundaries (different subnets). An mDNS gateway provides transport for service discovery across Layer 3 boundaries by filtering, caching, and redistributing services from one Layer 3 domain (subnet) to another. Prior to implementation of this feature, mDNS was limited in scope to within a subnet because of the use of link-local scoped multicast addresses. This feature enhances Bring Your Own Device (BYOD).

Related Topics

Configuring the Service List (CLI), on page 387
Example: Creating a Service-List, Applying a Filter and Configuring Parameters, on page 396
Enabling mDNS Gateway and Redistributing Services (CLI), on page 390
Example: Specify Alternative Source Interface for Outgoing mDNS Packets, on page 395
Example: Redistribute Service Announcements, on page 395
Example: Disable Bridging of mDNS Packets to Wireless Clients, on page 395
Example: Enabling mDNS Gateway and Redistributing Services, on page 396
Example: Global mDNS Configuration, on page 396
Example: Interface mDNS Configuration, on page 397

mDNS Gateway and Subnets

You need to enable an mDNS gateway for service discovery to operate across subnets. You can enable mDNS gateway for a device or for an interface.

Note You need to configure service routing globally before configuring at the interface level.

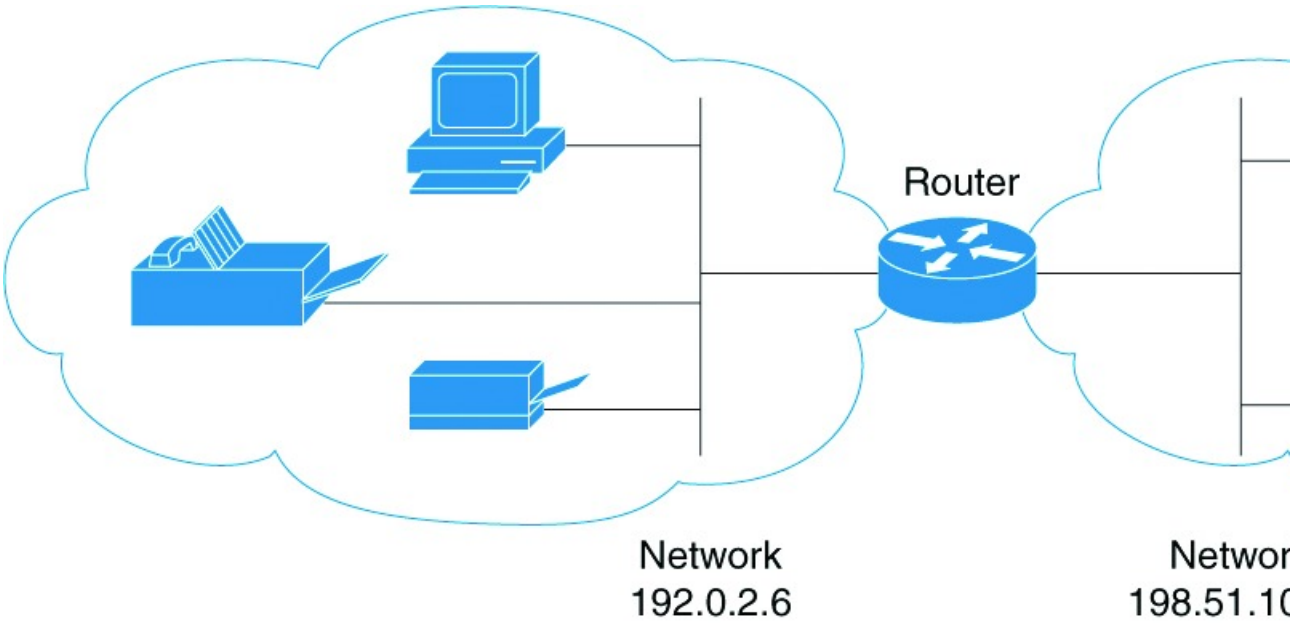
After the device or interface is enabled, you can redistribute service discovery information across subnets. You can create service policies and apply filters on either incoming service discovery information (called IN-bound filtering) or outgoing service discovery information (called OUT-bound filtering).

Note If redistribution is enabled globally, global configuration is given higher priority than interface configuration.

Figure 28: Sample Networking Scenario

For example, if the mDNS gateway functionality is enabled on the router in this figure, then service information can be sent from one subnet to another and vice-versa. For example, the printer and fax service information being advertised in the network with IP address 192.0.2.6 are redistributed to the network with IP address 198.51.100.4. The printer and fax service information in the network with IP address 192.0.2.6 is learned by

mDNS-enabled hosts and devices in the other network.



Filtering

After configuring the mDNS gateway and subnets, you can filter services that you want to redistribute. While creating a service list, the **permit** or **deny** command options are used:

- The **permit** command option allows you to permit or transport specific service list information.
- The **deny** option allows you to deny service list information that is available to be transported to other subnets.

You need to include a sequence number when using the **permit** or **deny** command option. The same service list name can be associated with multiple sequence numbers and each sequence number will be mapped to a rule.

Note If no filters are configured, then the default action is to deny service list information to be transported through the device or interface.

Query is another option provided when creating service lists. You can create queries using a service list. If you want to browse for a service, then active queries can be used. This function is helpful to keep the records refreshed in the cache.

Note Active queries can only be used globally and cannot be used at the interface level.

A service end-point (such as a printer or fax) sends unsolicited announcements when a service starts up. After that, it sends unsolicited announcements whenever a network change event occurs (such as an interface coming up or going down). The device always respond to queries.

After creating a service list and using the **permit** or **deny** command options, you can filter using match statements (commands) based on *service-instance*, *service-type*, or *message-type* (announcement or query).

Related Topics

Configuring the Service List (CLI), on page 387
Example: Creating a Service-List, Applying a Filter and Configuring Parameters, on page 396
Enabling mDNS Gateway and Redistributing Services (CLI), on page 390
Example: Specify Alternative Source Interface for Outgoing mDNS Packets, on page 395
Example: Redistribute Service Announcements, on page 395
Example: Disable Bridging of mDNS Packets to Wireless Clients, on page 395
Example: Enabling mDNS Gateway and Redistributing Services, on page 396
Example: Global mDNS Configuration, on page 396
Example: Interface mDNS Configuration, on page 397

How to Configure the Service Discovery Gateway

Configuring the Service List (CLI)

This procedure describes how to create a service list, apply a filter for the service list, and configure parameters for the service list name.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

Step 3	**service-list mdns-sd** *service-list-name* {**deny** *sequence-number* | **permit** *sequence-number* | **query**}
	Example:
	`Switch(config)# service-list mdns-sd sl1 permit 3`
	`Switch(config)# service-list mdns-sd sl4`
		Enters mDNS service discovery service list mode. In this mode, you can:
		• Create a service list and apply a filter on the service list according to the **permit** or **deny** option applied to the sequence number.
		• Create a service list and associate a query for the service list name if the **query** option is used.

	Command or Action	Purpose
	`query`	**Note** The sequence number sets the priority of the rule. A rule with a lower sequence number is selected first and the service announcement or query is allowed or denied accordingly. You define the sequence number as per your network requirements.
Step 4	**match message-type** {**announcement** | **any** | **query**} **Example:** `Switch(config-mdns-sd-sl)# match message-type announcement`	(Optional) Sets the message type to match. You can match the following message types: • announcement • any • query These commands configure the parameters for the service list name that is created in step 2. If the **match message-type** is an announcement, then the service list rule only allows service advertisements or announcements for the device. If the **match message-type** is a query, then only a query from the client for a certain service in the network is allowed. Multiple service maps of the same name with different sequence numbers can be created and the evaluation of the filters will be ordered on the sequence number. Service lists are an ordered sequence of individual statements, each one has a permit or deny result. Evaluation of service list consists of a list scan, in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is stopped once the first statement match is found and an action permit/deny associated with the statement match is performed. The default action after scanning through the entire list is to deny. **Note** You cannot use the **match** command if you have used the **query** option in the previous step. The **match** command can be used only for the **permit** or **deny** option.
Step 5	**match service-instance** { *LINE* } **Example:**	(Optional) Sets the service instance to match.

	Command or Action	Purpose
	`Switch(config-mdns-sd-sl)## match service-instance servInst 1`	This command configures the parameters for the service list name that is created in step 2. **Note** You cannot use the **match** command if you have used the **query** option in the previous step. The **match** command can be used only for the **permit** or **deny** option.
Step 6	**match service-type** {*LINE* } **Example:** `Switch(config-mdns-sd-sl)# match service-type _ipp._tcp`	(Optional) Sets the value of the mDNS service type string to match. This command configures the parameters for the service list name that is created in step 2. **Note** You cannot use the **match** command if you have used the **query** option in the previous step. The **match** command can be used only for the **permit** or **deny** option.
Step 7	**end** **Example:** `Switch(config-mdns-sd-sl)# end`	Returns to privileged EXEC mode.

What to do next

Proceed to enable the mDNS gateway and redistribution of services.

Related Topics

Service Discovery Gateway , on page 385
Filtering, on page 386
Example: Creating a Service-List, Applying a Filter and Configuring Parameters, on page 396

Configuring the Service List (GUI)

Procedure

Step 1 Choose **Configuration** > **Controller** > **mDNS** > **Static Service**.

Step 2 Click **Create Service**.
The **Service List** > **Create Service** page is displayed.

Step 3 In the **Service List Name** text box, enter the service list name.

Step 4 From the **Service rule** drop-down list, choose from the following options:

- **permit**—permits the service list.

- **deny**—denies the service list.

Step 5 In the **Sequence number** text box, enter the priority of the rule.

A rule with a lower sequence number is selected first and the service announcement or query is allowed or denied accordingly. You define the sequence number as per your network requirements.

Step 6 From the **Message type** drop-down list, choose the message type to match from the following options:

- **announcement**—The service list rule allows only service advertisements or announcements for the device.
- **query**—The service list rule allows only a query from the client for a service in the network.
- **any**—The service list rule allows any type of message.

Multiple service maps of the same name with different sequence numbers can be created and the evaluation of the filters will be ordered on the sequence number. Service lists are an ordered sequence of individual statements, each one has a permit or deny result. Evaluation of service list consists of a list scan, in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is stopped once the first statement match is found and an action permit/deny associated with the statement match is performed. The default action after scanning through the entire list is to deny.

Step 7 In the **Service instance** text box, enter the service instance to match.

Step 8 In the **Custom** text box, enter the mDNS service type string to match.

The **Learned Service** box shows the services that are added after enabling the learned service type configured by navigating to **Configuration** > **Controller** > **mDNS** > **Global**. For example, _roap._tcp.local.

The **Selected Service** box shows the learned service that you have selected for an mDNS service.

Step 9 Click **Apply**.

Step 10 Click **Save Configuration**.

What to do next

Proceed to enable the mDNS gateway and redistribution of services.

Enabling mDNS Gateway and Redistributing Services (CLI)

After enabling mDNS gateway for a device, you can apply filters (apply IN-bound filtering or OUT-bound filtering) and active queries by using **service-policy** and **service-policy-query** commands, respectively. You can redistribute services and service announcements using the **redistribute mdns-sd** command, and set some part of the system memory for cache using the **cache-memory-max** command.

Note By default, mDNS gateway is disabled on all interfaces.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Switch> enable`	
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**service-routing mdns-sd** **Example:** `Switch (config)# service-routing mdns-sd`	Enables mDNS gateway functionality for a device and enters multicast DNS configuration (config-mdns) mode. **Note** This command enables the mDNS function globally. **Note** Enter the **service-routing mdns-sd source-interface** *if-name* command in either global-config or interface-config mode, to specify an alternate source interface for outgoing mDNS packets, so its IP address can be used when there is none configured on the outgoing interface.
Step 4	**service-policy** *service-policy-name* {**IN** | **OUT**} **Example:** `Switch (config-mdns)# service-policy serv-pol1 IN`	(Optional) For a service list, applies a filter on incoming service discovery information (IN-bound filtering) or outgoing service discovery information (OUT-bound filtering).
Step 5	**redistribute mdns-sd** **Example:** `Switch (config-mdns)# redistribute mdns-sd`	(Optional) Redistributes services or service announcements across subnets. **Note** If redistribution is enabled globally, global configuration is given higher priority than interface configuration.
Step 6	**cache-memory-max** *cache-config-percentage* **Example:** `Switch (config-mdns)# cache-memory-max 20`	(Optional) Sets some part of the system memory (in percentage) for cache. **Note** By default, 10 percent of the system memory is set aside for cache. You can override the default value by using this command.

	Command or Action	Purpose
Step 7	**service-policy-query** *service-list-query-name service-list-query-periodicity* **Example:** `Switch (config-mdns)# service-policy-query sl-query1 100`	(Optional) Configures service list-query periodicity.
Step 8	**exit** **Example:** `Switch (config-mdns)#exit`	(Optional) Returns to global configuration mode.
Step 9	**wireless multicast** **Example:** `Switch (config)# wireless multicast`	(Optional) Enables wireless Ethernet multicast support.
Step 10	**no wireless mdns-bridging** **Example:** `Switch (config)# no wireless mdns-bridging`	(Optional) Disables bridging of mDNS packets to wireless clients.
Step 11	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Related Topics

Service Discovery Gateway , on page 385
Filtering, on page 386
Example: Specify Alternative Source Interface for Outgoing mDNS Packets, on page 395
Example: Redistribute Service Announcements, on page 395
Example: Disable Bridging of mDNS Packets to Wireless Clients, on page 395
Example: Enabling mDNS Gateway and Redistributing Services, on page 396
Example: Global mDNS Configuration, on page 396
Example: Interface mDNS Configuration, on page 397

Configuring Interface Service Rules (GUI)

Procedure

Step 1 Choose **Configuration** > **Controller** > **mDNS** > **Interface**.

Step 2 Click an interface name.

The **Interface Service Rules** page is displayed.

Step 3 From the **Service Policy IN** drop-down list, choose the service policy that should be applied for incoming mDNS messages.

Step 4 From the **Service Policy OUT** drop-down list, choose the service policy that should be applied for outgoing mDNS messages.

Step 5 Select or unselect the **Redistribution** check box to enable or disable redistribution of service announcements received on one interface over all the interfaces or over a specific interface.

Step 6 Check **Enable** to enable a self designated gateway for the interface.

Step 7 Enter values for proximity- **maximum service** option and **service list active query** in the text box. The value ranges from 1 to 100 for **maximum service**.

Step 8 To create a new **Service Type**, select **Create New** from the drop-down box.

Step 9 Click **Apply**.

Step 10 Click **Save Configuration**.

Configuring mDNS Global Rules (GUI)

Procedure

Step 1 Choose **Configuration** > **Controller** > **mDNS** > **Global**.

Step 2 Select the **mDNS gateway** check box.

Step 3 Follow these steps to configure downstream rules that include service lists and service rules that you can apply for all the downstream traffic on the switch.

a) Click the **Down Stream Rules** tab.

b) From the **Service List Name** drop-down list, choose **Create New**. In the **Service List Name** box, enter a name.

c) Click **Add** to add a service rule, and follow on-screen instructions to specify the service rules that include **Action**, **Message Type**, **Service Instance**, and **Service Type**.

See the online help for detailed descriptions of the fields.

Step 4 Follow these steps to configure the upstream rules that include service lists and service rules that you can apply for all the upstream traffic on the switch.

a) Click the **Up Stream Rules** tab.

b) From the **Service List Name** drop-down list, choose **Create New**. In the **New Service List Name** box, enter a name.

c) Click **Add** to add a service rule, and follow on-screen instructions to specify the service rules that include **Action**, **Message Type**, **Service Instance**, and **Service Type**.

See the online help for detailed descriptions of the fields.

Step 5 Follow these steps to configure the switch as designated gateway and apply proximity rules:

a) Click the **Advanced** tab.

b) Select or unselect the **Self Designated Gateway** check box.

c) Under **Proximity**, in the **Max Services Option** box, enter the maximum number of devices supported with a particular service type that are in proximity. The valid range is between 1 and 100.

d) From the **Service List Active Query** drop-down list, choose the services that are filtered for proximity.

You can create a custom service list, by choosing **Create New** and then specifying the service list name.

e) Click **New** to add a service type, and from the **Service Type** drop-down list, choose the service type to be added, and click **OK**.

See the online help for detailed descriptions of the fields.

Step 6 From the **Learn Service** drop-down list, choose from the following options:

- **Enable**— Allows the switch to learn all the announced services. It is used to learn services by enabling all announcement/queries by using Service Policy IN of type GUI-permit-all and in Service Policy OUT of type GUI-deny-all.
- **Disable**— Denies all the traffics IN and OUT. It is used to deny services by disabling all announcement/queries by using Service Policy IN of type GUI-deny-all and in Service Policy OUT of type GUI-deny-all.
- **Custom**— You can set your own IN and OUT policy. It allows you to define a custom service list.

Step 7 Click **Apply**.

Step 8 Click **Save Configuration**.

Monitoring Service Discovery Gateway

Table 22: Monitoring Service Discovery Gateway

Command	Purpose
show mdns requests [**detail** | **name** *record-name*| **type** *record-type* [**name** *record-name*]]	This command displays information for outstanding mDNS requests, including record name and record type information.
show mdns cache [**interface** *type number* | **name** *record-name* [**type** *record-type*]| **type** *record-type*]	This command displays mDNS cache information.
show mdns statistics {**all** | **service-list** *list-name* | **service-policy** {**all** | **interface** *type number* }}	This command displays mDNS statistics.

Configuration Examples

Example: Specify Alternative Source Interface for Outgoing mDNS Packets

The following example displays how to specify an alternate source interface for outgoing mDNS packets, so its IP address can be used when there is none configured on the outgoing interface.

```
Switch(config)# service-routing mdns-sd
Switch(config-mdns)# source-interface if-name
```

Related Topics

Enabling mDNS Gateway and Redistributing Services (CLI), on page 390
Service Discovery Gateway , on page 385
Filtering, on page 386

Example: Redistribute Service Announcements

The following example displays how to redistribute service announcements received on one interface over all the interfaces or over a specific interface.

```
Switch(config)# service-routing mdns-sd
Switch(config-mdns)# Redistribute mdns-sd if-name
```

Related Topics

Enabling mDNS Gateway and Redistributing Services (CLI), on page 390
Service Discovery Gateway , on page 385
Filtering, on page 386

Example: Disable Bridging of mDNS Packets to Wireless Clients

The following example displays how to disable bridging of mDNS packets to wireless clients.

```
Switch(config)# wireless multicast
Switch(config)# no wireless mdns-bridging
```

Related Topics

Enabling mDNS Gateway and Redistributing Services (CLI), on page 390
Service Discovery Gateway , on page 385
Filtering, on page 386

Example: Creating a Service-List, Applying a Filter and Configuring Parameters

The following example shows the creation of a service-list sl1. The **permit** command option is being applied on sequence number 3 and all services with message-type announcement are filtered and available for transport across various subnets associated with the device.

```
Switch# configure terminal
Switch(config)# service-list mdns-sd sl1 permit 3
Switch(config-mdns-sd-sl)#match message-type announcement
Switch(config-mdns)# exit
```

Related Topics

Configuring the Service List (CLI), on page 387
Service Discovery Gateway , on page 385
Filtering, on page 386

Example: Enabling mDNS Gateway and Redistributing Services

The following example shows how to enable an mDNS gateway for a device and enable redistribution of services across subnets. IN-bound filtering is applied on the service-list serv-pol1. Twenty percent of system memory is made available for cache and service-list-query periodicity is configured at 100 seconds.

```
Switch# configure terminal
Switch# service-routing mdns-sd
Switch(config-mdns)# service-policy serv-pol1 IN
Switch(config-mdns)# redistribute mdns-sd
Switch(config-mdns)# cache-memory-max 20
Switch(config-mdns)# service-policy-query sl-query1 100
Switch(config-mdns)# exit
```

Related Topics

Enabling mDNS Gateway and Redistributing Services (CLI), on page 390
Service Discovery Gateway , on page 385
Filtering, on page 386

Example: Global mDNS Configuration

The following example displays how to globally configure mDNS.

```
Switch# configure terminal
Switch(config)# service-list mdns-sd mypermit-all permit 10
Switch(config-mdns-sd-sl)# exit
Switch(config)# service-list mdns-sd querier query
Switch(config-mdns-sd-sl)# service-type _dns._udp
Switch(config-mdns-sd-sl)# end
Switch# configure terminal
Switch(config)# service-routing mdns-sd
Switch(config-mdns)# service-policy mypermit-all IN
Switch(config-mdns)# service-policy mypermit-all OUT
```

Related Topics

Enabling mDNS Gateway and Redistributing Services (CLI), on page 390
Service Discovery Gateway , on page 385
Filtering, on page 386

Example: Interface mDNS Configuration

The following example displays how to configure mDNS for an interface.

```
Switch(config)#interface Vlan136
Switch(config-if)# description *** Mgmt VLAN ***
Switch(config-if)# ip address 9.7.136.10 255.255.255.0
Switch(config-if)# ip helper-address 9.1.0.100
Switch(config-if)# service-routing mdns-sd
Switch(config-if-mdns-sd)#  service-policy mypermit-all IN
Switch(config-if-mdns-sd)# service-policy mypermit-all OUT
Switch(config-if-mdns-sd)#  service-policy-query querier 60
```

Related Topics

Enabling mDNS Gateway and Redistributing Services (CLI), on page 390
Service Discovery Gateway , on page 385
Filtering, on page 386

Monitoring Service Cache (GUI)

Click **Monitor > Controller > mDNS > Service Cache** to view domain names and other details of the service providers.

Each service advertisement contains a record that maps the domain name of the service provider to the IP address. The details of the following parameters is displayed:

Name	Displays the hostname assigned to each service provider machine.
VLAN ID	Displays the VLAN ID of the service provider.
MAC ID	Displays the MAC address of the service provider machine.
TTL	Displays the Time to Live (TTL) value in seconds that determines the validity of the service offered by the service provider. The service provider is removed from the Switchwhen the TTL expires.
Remaining	Displays the time left in seconds before the service provider is removed from the Switch.

Type	Displays the service type record. Values are as follow: • PTR • TXT • SRV
RR Record Data	Displays IP addresses, service names of the announced services.

Monitoring Static Service Cache (GUI)

Click **Monitor > Controller > mDNS > Static Service Cache** to view domain names and other details of the service providers.

Each service advertisement contains a record that maps the domain name of the service provider to the IP address. The details of the following parameters is displayed:

Name	Displays the hostname assigned to each service provider machine.
VLAN ID	Displays the VLAN ID of the service provider.
MAC ID	Displays the MAC address of the service provider machine.
TTL	Displays the Time to Live (TTL) value in seconds that determines the validity of the service offered by the service provider. The service provider is removed from the Switchwhen the TTL expires.
Remaining	Displays the time left in seconds before the service provider is removed from the Switch.
Type	Displays the service type record. Values are as follow: • PTR • TXT • SRV
RR Record Data	Displays IP addresses, service names of the announced services.

Where to Go Next for Configuring Services Discovery Gateway

You can configure the following:

Additional References

Related Documents

Related Topic	Document Title
Configuring DNS	*IP Addressing: DNS Configuration Guide, Cisco IOS XE Release 3SE*
DNS conceptual information	'Information About DNS' section in *IP Addressing: DNS Configuration Guide, Cisco IOS XE Release 3SE*
Platform-independent configuration information	*IP Addressing: DNS Configuration Guide, Cisco IOS XE Release 3SE*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
RFC 6763	*DNS-Based Service Discovery*
Multicast DNS Internet-Draft	Multicast

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

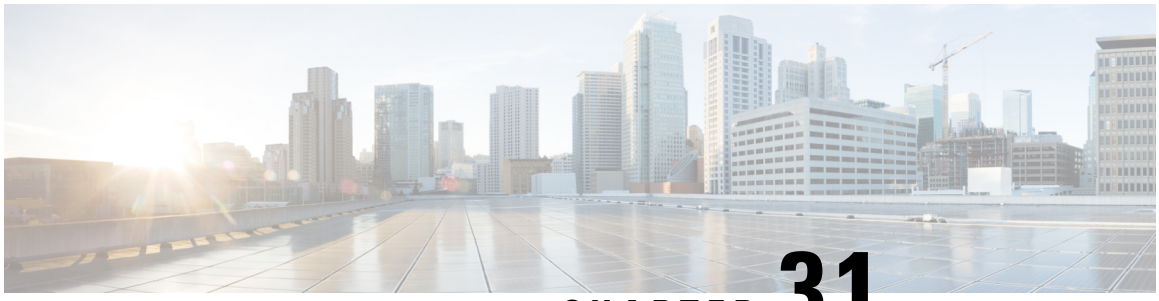
Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for Services Discovery Gateway

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.

PART VIII

Network Management



CHAPTER 31

Configuring Cisco IOS Configuration Engine

Prerequisites for Configuring the Configuration Engine

- Obtain the name of the configuration engine instance to which you are connecting.
- Because the CNS uses both the event bus and the configuration server to provide configurations to devices, you must define both ConfigID and Device ID for each configured switch.
- All switches configured with the **cns config partial** global configuration command must access the event bus. The DeviceID, as originated on the switch, must match the DeviceID of the corresponding switch definition in the Cisco Configuration Engine. You must know the hostname of the event bus to which you are connecting.

Restrictions for Configuring the Configuration Engine

- Within the scope of a single instance of the configuration server, no two configured switches can share the same value for ConfigID.
- Within the scope of a single instance of the event bus, no two configured switches can share the same value for DeviceID.

Information About Configuring the Configuration Engine

Cisco Configuration Engine Software

The Cisco Configuration Engine is network management utility software that acts as a configuration service for automating the deployment and management of network devices and services. Each Cisco Configuration Engine manages a group of Cisco devices (switches and routers) and the services that they deliver, storing their configurations and delivering them as needed. The Cisco Configuration Engine automates initial configurations and configuration updates by generating device-specific configuration changes, sending them to the device, executing the configuration change, and logging the results.

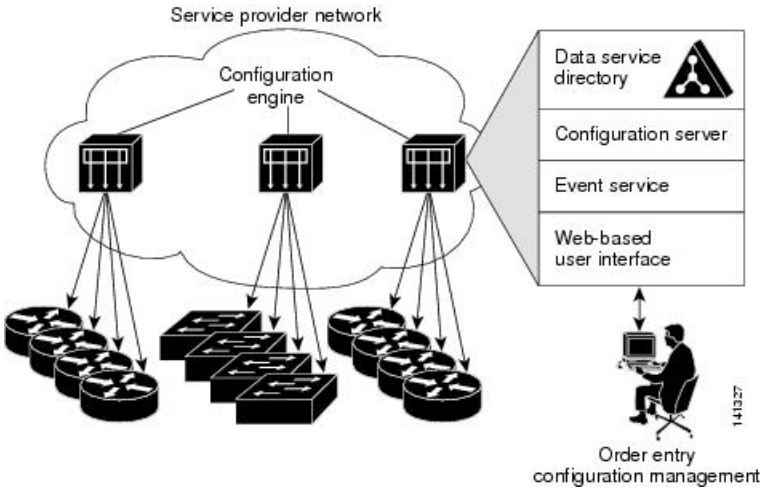
The Cisco Configuration Engine supports standalone and server modes and has these Cisco Networking Services (CNS) components:

- Configuration service:
  - Web server
  - File manager
  - Namespace mapping server
- Event service (event gateway)
- Data service directory (data models and schema)

Note Support for Cisco Configuration Engine will be deprecated in future releases. Use the configuration described in Cisco Plug and Play Feature Guide .

In standalone mode, the Cisco Configuration Engine supports an embedded directory service. In this mode, no external directory or other data store is required. In server mode, the Cisco Configuration Engine supports the use of a user-defined external directory.

Figure 29: Cisco Configuration Engine Architectural Overview



Configuration Service

The Configuration Service is the core component of the Cisco Configuration Engine. It consists of a Configuration Server that works with Cisco IOS CNS agents on the switch. The Configuration Service delivers device and service configurations to the switch for initial configuration and mass reconfiguration by logical groups. Switches receive their initial configuration from the Configuration Service when they start up on the network for the first time.

The Configuration Service uses the CNS Event Service to send and receive configuration change events and to send success and failure notifications.

The Configuration Server is a web server that uses configuration templates and the device-specific configuration information stored in the embedded (standalone mode) or remote (server mode) directory.

Configuration templates are text files containing static configuration information in the form of CLI commands. In the templates, variables are specified by using Lightweight Directory Access Protocol (LDAP) URLs that reference the device-specific configuration information stored in a directory.

The Cisco IOS agent can perform a syntax check on received configuration files and publish events to show the success or failure of the syntax check. The configuration agent can either apply configurations immediately or delay the application until receipt of a synchronization event from the configuration server.

Event Service

The Cisco Configuration Engine uses the Event Service for receipt and generation of configuration events. The Event Service consists of an event agent and an event gateway. The event agent is on the switch and facilitates the communication between the switch and the event gateway on the Cisco Configuration Engine.

The Event Service is a highly capable publish-and-subscribe communication method. The Event Service uses subject-based addressing to send messages to their destinations. Subject-based addressing conventions define a simple, uniform namespace for messages and their destinations.

NameSpace Mapper

The Cisco Configuration Engine includes the NameSpace Mapper (NSM) that provides a lookup service for managing logical groups of devices based on application, device or group ID, and event.

Cisco IOS devices recognize only event subject-names that match those configured in Cisco IOS software; for example, cisco.cns.config.load. You can use the namespace mapping service to designate events by using any desired naming convention. When you have populated your data store with your subject names, NSM changes your event subject-name strings to those known by Cisco IOS.

For a subscriber, when given a unique device ID and event, the namespace mapping service returns a set of events to which to subscribe. Similarly, for a publisher, when given a unique group ID, device ID, and event, the mapping service returns a set of events on which to publish.

Cisco Networking Services IDs and Device Hostnames

The Cisco Configuration Engine assumes that a unique identifier is associated with each configured switch. This unique identifier can take on multiple synonyms, where each synonym is unique within a particular namespace. The event service uses namespace content for subject-based addressing of messages.

The Cisco Configuration Engine intersects two namespaces, one for the event bus and the other for the configuration server. Within the scope of the configuration server namespace, the term *ConfigID* is the unique identifier for a device. Within the scope of the event bus namespace, the term *DeviceID* is the CNS unique identifier for a device.

ConfigID

Each configured switch has a unique ConfigID, which serves as the key into the Cisco Configuration Engine directory for the corresponding set of switch CLI attributes. The ConfigID defined on the switch must match the ConfigID for the corresponding switch definition on the Cisco Configuration Engine.

The ConfigID is fixed at startup time and cannot be changed until the device restarts, even if the switch hostname is reconfigured.

DeviceID

Each configured switch participating on the event bus has a unique DeviceID, which is analogous to the switch source address so that the switch can be targeted as a specific destination on the bus.

The origin of the DeviceID is defined by the Cisco IOS hostname of the switch. However, the DeviceID variable and its usage reside within the event gateway adjacent to the switch.

The logical Cisco IOS termination point on the event bus is embedded in the event gateway, which in turn functions as a proxy on behalf of the switch. The event gateway represents the switch and its corresponding DeviceID to the event bus.

The switch declares its hostname to the event gateway immediately after the successful connection to the event gateway. The event gateway couples the DeviceID value to the Cisco IOS hostname each time this connection is established. The event gateway retains this DeviceID value for the duration of its connection to the switch.

Hostname and DeviceID

The DeviceID is fixed at the time of the connection to the event gateway and does not change even when the switch hostname is reconfigured.

When changing the switch hostname on the switch, the only way to refresh the DeviceID is to break the connection between the switch and the event gateway. For instructions on refreshing DeviceIDs, see "Related Topics."

When the connection is reestablished, the switch sends its modified hostname to the event gateway. The event gateway redefines the DeviceID to the new value.

Caution When using the Cisco Configuration Engine user interface, you must first set the DeviceID field to the hostname value that the switch acquires *after*, not *before*, and you must reinitialize the configuration for your Cisco IOS CNS agent. Otherwise, subsequent partial configuration command operations may malfunction.

Hostname, DeviceID, and ConfigID

In standalone mode, when a hostname value is set for a switch, the configuration server uses the hostname as the DeviceID when an event is sent on hostname. If the hostname has not been set, the event is sent on the cn=<*value*> of the device.

In server mode, the hostname is not used. In this mode, the unique DeviceID attribute is always used for sending an event on the bus. If this attribute is not set, you cannot update the switch.

These and other associated attributes (tag value pairs) are set when you run **Setup** on the Cisco Configuration Engine.

Cisco IOS CNS Agents

The CNS event agent feature allows the switch to publish and subscribe to events on the event bus and works with the Cisco IOS CNS agent. These agents, embedded in the switch Cisco IOS software, allow the switch to be connected and automatically configured.

Initial Configuration

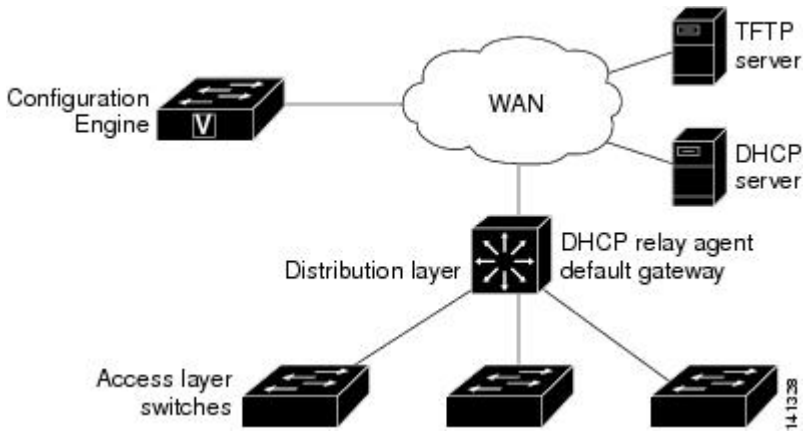
When the switch first comes up, it attempts to get an IP address by broadcasting a Dynamic Host Configuration Protocol (DHCP) request on the network. Assuming there is no DHCP server on the subnet, the distribution switch acts as a DHCP relay agent and forwards the request to the DHCP server. Upon receiving the request, the DHCP server assigns an IP address to the new switch and includes the Trivial File Transfer Protocol (TFTP) server Internet Protocol (IP) address, the path to the bootstrap configuration file, and the default gateway IP address in a unicast reply to the DHCP relay agent. The DHCP relay agent forwards the reply to the switch.

The switch automatically configures the assigned IP address on interface VLAN 1 (the default) and downloads the bootstrap configuration file from the TFTP server. Upon successful download of the bootstrap configuration file, the switch loads the file in its running configuration.

The Cisco IOS CNS agents initiate communication with the Configuration Engine by using the appropriate ConfigID and EventID. The Configuration Engine maps the Config ID to a template and downloads the full configuration file to the switch.

The following figure shows a sample network configuration for retrieving the initial bootstrap configuration file by using DHCP-based autoconfiguration.

Figure 30: Initial Configuration



Incremental (Partial) Configuration

After the network is running, new services can be added by using the Cisco IOS CNS agent. Incremental (partial) configurations can be sent to the switch. The actual configuration can be sent as an event payload by way of the event gateway (push operation) or as a signal event that triggers the switch to initiate a pull operation.

The switch can check the syntax of the configuration before applying it. If the syntax is correct, the switch applies the incremental configuration and publishes an event that signals success to the configuration server. If the switch does not apply the incremental configuration, it publishes an event showing an error status. When the switch has applied the incremental configuration, it can write it to nonvolatile random-access memory (NVRAM) or wait until signaled to do so.

Synchronized Configuration

When the switch receives a configuration, it can defer application of the configuration upon receipt of a write-signal event. The write-signal event tells the switch not to save the updated configuration into its NVRAM. The switch uses the updated configuration as its running configuration. This ensures that the switch configuration is synchronized with other network activities before saving the configuration in NVRAM for use at the next reboot.

Automated CNS Configuration

To enable automated CNS configuration of the switch, you must first complete the prerequisites listed in this topic. When you complete them, power on the switch. At the **setup** prompt, do nothing; the switch begins the initial configuration. When the full configuration file is loaded on your switch, you do not need to do anything else.

For more information on what happens during initial configuration, see "Related Topics."

Table 23: Prerequisites for Enabling Automatic Configuration

Device	Required Configuration
Access switch	Factory default (no configuration file)

Device	Required Configuration
Distribution switch	• IP helper address • Enable DHCP relay agent[2] • IP routing (if used as default gateway)
DHCP server	• IP address assignment • TFTP server IP address • Path to bootstrap configuration file on the TFTP server • Default gateway IP address
TFTP server	• A bootstrap configuration file that includes the CNS configuration commands that enable the switch to communicate with the Configuration Engine • The switch configured to use either the switch MAC address or the serial number (instead of the default hostname) to generate the ConfigID and EventID • The CNS event agent configured to push the configuration file to the switch
CNS Configuration Engine	One or more templates for each type of device, with the ConfigID of the device mapped to the template.

[2] A DHCP Relay is needed only when the DHCP Server is on a different subnet from the client.

How to Configure the Configuration Engine

Enabling the CNS Event Agent

Note You must enable the CNS event agent on the switch before you enable the CNS configuration agent.

Follow these steps to enable the CNS event agent on the switch.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**cns event** {*hostname* | *ip-address*} [*port-number*] [[**keepalive** *seconds retry-count*] [**failover-time** *seconds*] [**reconnect-time** *time*] | **backup**] **Example:** `Switch(config)# cns event 10.180.1.27 keepalive 120 10`	Enables the event agent, and enters the gateway parameters. • For {*hostname* | *ip-address*}, enter either the hostname or the IP address of the event gateway. • (Optional) For *port number*, enter the port number for the event gateway. The default port number is 11011. • (Optional) For **keepalive** *seconds*, enter how often the switch sends keepalive messages. For *retry-count*, enter the number of unanswered keepalive messages that the switch sends before the connection is terminated. The default for each is 0. • (Optional) For **failover-time** *seconds*, enter how long the switch waits for the primary gateway route after the route to the backup gateway is established. • (Optional) For **reconnect-time** *time*, enter the maximum time interval that the switch waits before trying to reconnect to the event gateway. • (Optional) Enter **backup** to show that this is the backup gateway. (If omitted, this is the primary gateway.) **Note** Though visible in the command-line help string, the **encrypt** and the **clock-timeout** *time* keywords are not supported.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:**	Verifies your entries.

	Command or Action	Purpose
	`Switch# show running-config`	
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

To verify information about the event agent, use the **show cns event connections** command in privileged EXEC mode.

To disable the CNS event agent, use the **no cns event** { *ip-address* | *hostname* } global configuration command.

Enabling the Cisco IOS CNS Agent

Follow these steps to enable the Cisco IOS CNS agent on the switch.

Before you begin

You must enable the CNS event agent on the switch before you enable this agent.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**cns config initial** {*hostname* | *ip-address*} [*port-number*] **Example:** `Switch(config)# cns config initial 10.180.1.27 10`	Enables the Cisco IOS CNS agent, and enters the configuration server parameters. • For {*hostname* | *ip-address*}, enter either the hostname or the IP address of the configuration server. • (Optional) For *port number*, enter the port number for the configuration server.

	Command or Action	Purpose
		This command enables the Cisco IOS CNS agent and initiates an initial configuration on the switch.
Step 4	**cns config partial** {*hostname* | *ip-address*} [*port-number*] **Example:** `Switch(config)# cns config partial 10.180.1.27 10`	Enables the Cisco IOS CNS agent, and enters the configuration server parameters. • For {*hostname* | *ip-address*}, enter either the hostname or the IP address of the configuration server. • (Optional) For *port number*, enter the port number for the configuration server. Enables the Cisco IOS CNS agent and initiates a partial configuration on the switch.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.
Step 8	Start the Cisco IOS CNS agent on the switch.	

What to do next

You can now use the Cisco Configuration Engine to remotely send incremental configurations to the switch.

Enabling an Initial Configuration for Cisco IOS CNS Agent

Follow these steps to enable the CNS configuration agent and initiate an initial configuration on the switch.

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Switch> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**cns template connect** *name* **Example:** `Switch(config)# cns template connect template-dhcp`	Enters CNS template connect configuration mode, and specifies the name of the CNS connect template.
Step 4	**cli** *config-text* **Example:** `Switch(config-tmpl-conn)# cli ip address dhcp`	Enters a command line for the CNS connect template. Repeat this step for each command line in the template.
Step 5	Repeat Steps 3 to 4 to configure another CNS connect template.	
Step 6	**exit** **Example:** `Switch(config)# exit`	Returns to global configuration mode.
Step 7	**cns connect** *name* [**retries** *number*] [**retry-interval** *seconds*] [**sleep** *seconds*] [**timeout** *seconds*] **Example:** `Switch(config)# cns connect dhcp`	Enters CNS connect configuration mode, specifies the name of the CNS connect profile, and defines the profile parameters. The switch uses the CNS connect profile to connect to the Configuration Engine. • Enter the *name* of the CNS connect profile. • (Optional) For **retries** *number*, enter the number of connection retries. The range is 1 to 30. The default is 3. • (Optional) For **retry-interval** *seconds*, enter the interval between successive connection attempts to the Configuration Engine. The range is 1 to 40 seconds. The default is 10 seconds. • (Optional) For **sleep** *seconds*, enter the amount of time before which the first

	Command or Action	Purpose
		connection attempt occurs. The range is 0 to 250 seconds. The default is 0. • (Optional) For **timeout** *seconds*, enter the amount of time after which the connection attempts end. The range is 10 to 2000 seconds. The default is 120.
Step 8	**discover** {**controller** *controller-type* | **dlci** [**subinterface** *subinterface-number*] | **interface** [*interface-type*] | **line** *line-type*} **Example:** `Switch(config-cns-conn)# discover interface gigabitethernet`	Specifies the interface parameters in the CNS connect profile. • For **controller** *controller-type*, enter the controller type. • For **dlci**, enter the active data-link connection identifiers (DLCIs). (Optional) For **subinterface** *subinterface-number*, specify the point-to-point subinterface number that is used to search for active DLCIs. • For **interface** [*interface-type*], enter the type of interface. • For **line** *line-type*, enter the line type.
Step 9	**template** *name* [... *name*] **Example:** `Switch(config-cns-conn)# template template-dhcp`	Specifies the list of CNS connect templates in the CNS connect profile to be applied to the switch configuration. You can specify more than one template.
Step 10	Repeat Steps 8 to 9 to specify more interface parameters and CNS connect templates in the CNS connect profile.	
Step 11	**exit** **Example:** `Switch(config-cns-conn)# exit`	Returns to global configuration mode.
Step 12	**hostname** *name* **Example:** `Switch(config)# hostname device1`	Enters the hostname for the switch.
Step 13	**ip route** *network-number* **Example:** `RemoteSwitch(config)# ip route`	(Optional) Establishes a static route to the Configuration Engine whose IP address is *network-number*.

	Command or Action	Purpose
	`172.28.129.22 255.255.255.255 11.11.11.1`	
Step 14	**cns id** *interface num* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**] **Example:** `RemoteSwitch(config)# cns id GigabitEthernet1/0/1 ipaddress`	(Optional) Sets the unique EventID or ConfigID used by the Configuration Engine. If you enter this command, do not enter the **cns id** {**hardware-serial** | **hostname** | **string** *string* | **udi**} [**event**] [**image**] command. • For *interface num*, enter the type of interface. For example, ethernet, group-async, loopback, or virtual-template. This setting specifies from which interface the IP or MAC address should be retrieved to define the unique ID. • For {**dns-reverse** | **ipaddress** | **mac-address**}, enter **dns-reverse** to retrieve the hostname and assign it as the unique ID, enter **ipaddress** to use the IP address, or enter **mac-address** to use the MAC address as the unique ID. • (Optional) Enter **event** to set the ID to be the event-id value used to identify the switch. • (Optional) Enter **image** to set the ID to be the image-id value used to identify the switch. **Note** If both the **event** and **image** keywords are omitted, the image-id value is used to identify the switch.
Step 15	**cns id** {**hardware-serial** | **hostname** | **string** *string* | **udi**} [**event**] [**image**] **Example:** `RemoteSwitch(config)# cns id hostname`	(Optional) Sets the unique EventID or ConfigID used by the Configuration Engine. If you enter this command, do not enter the **cns id** *interface num* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**] command. • For { **hardware-serial** | **hostname** | **string** *string* | **udi** }, enter **hardware-serial** to set the switch serial number as the unique ID, enter **hostname** (the default) to select the switch hostname as the unique ID, enter an arbitrary text string for **string** *string* as the unique ID, or enter **udi** to set the unique device identifier (UDI) as the unique ID.

	Command or Action	Purpose
Step 16	**cns config initial** {*hostname* | *ip-address*} [*port-number*] [**event**] [**no-persist**] [**page** *page*] [**source** *ip-address*] [**syntax-check**] **Example:** `RemoteSwitch(config)# cns config initial 10.1.1.1 no-persist`	Enables the Cisco IOS agent, and initiates an initial configuration. • For {*hostname* | *ip-address*}, enter the hostname or the IP address of the configuration server. • (Optional) For *port-number*, enter the port number of the configuration server. The default port number is 80. • (Optional) Enable **event** for configuration success, failure, or warning messages when the configuration is finished. • (Optional) Enable **no-persist** to suppress the automatic writing to NVRAM of the configuration pulled as a result of entering the **cns config initial** global configuration command. If the **no-persist** keyword is not entered, using the **cns config initial** command causes the resultant configuration to be automatically written to NVRAM. • (Optional) For **page** *page*, enter the web page of the initial configuration. The default is /Config/config/asp. • (Optional) Enter **source** *ip-address* to use for source IP address. • (Optional) Enable **syntax-check** to check the syntax when this parameter is entered. **Note** Though visible in the command-line help string, the **encrypt**, **status** *url*, and **inventory** keywords are not supported.
Step 17	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 18	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.

	Command or Action	Purpose
Step 19	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

To verify information about the configuration agent, use the **show cns config connections** command in privileged EXEC mode.

To disable the CNS Cisco IOS agent, use the **no cns config initial** { *ip-address* | *hostname* } global configuration command.

Refreshing DeviceIDs

Follow these steps to refresh a DeviceID when changing the hostname on the switch.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show cns config connections** **Example:** `Switch# show cns config connections`	Displays whether the CNS event agent is connecting to the gateway, connected, or active, and the gateway used by the event agent, its IP address and port number.
Step 3	Make sure that the CNS event agent is properly connected to the event gateway.	Examine the output of **show cns config connections** for the following: • Connection is active. • Connection is using the currently configured switch hostname. The DeviceID will be refreshed to correspond to the new hostname configuration using these instructions.
Step 4	**show cns event connections** **Example:** `Switch# show cns event connections`	Displays the event connection information for your switch.

	Command or Action	Purpose
Step 5	Record from the output of Step 4 the information for the currently connected connection listed below. You will be using the IP address and port number in subsequent steps of these instructions.	
Step 6	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 7	**no cns event** *ip-address port-number* **Example:** `Switch(config)# no cns event 172.28.129.22 2012`	Specifies the IP address and port number that you recorded in Step 5 in this command. This command breaks the connection between the switch and the event gateway. It is necessary to first break, then reestablish, this connection to refresh the DeviceID.
Step 8	**cns event** *ip-address port-number* **Example:** `Switch(config)# cns event 172.28.129.22 2012`	Specifies the IP address and port number that you recorded in Step 5 in this command. This command reestablishes the connection between the switch and the event gateway.
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 10	Make sure that you have reestablished the connection between the switch and the event connection by examining the output from **show cns event connections**.	
Step 11	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 12	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Enabling a Partial Configuration for Cisco IOS CNS Agent

Follow these steps to enable the Cisco IOS CNS agent and to initiate a partial configuration on the switch.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**cns config partial** {*ip-address* | *hostname*} [*port-number*] [**source** *ip-address*] **Example:** `Switch(config)# cns config partial 172.28.129.22 2013`	Enables the configuration agent, and initiates a partial configuration. • For {*ip-address* | *hostname*}, enter the IP address or the hostname of the configuration server. • (Optional) For *port-number*, enter the port number of the configuration server. The default port number is 80. • (Optional) Enter **source** *ip-address* to use for the source IP address. **Note** Though visible in the command-line help string, the **encrypt** keyword is not supported.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:**	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	`Switch# copy running-config startup-config`	

What to do next

To verify information about the configuration agent, use either the **show cns config stats** or the **show cns config outstanding** command in privileged EXEC mode.

To disable the Cisco IOS agent, use the **no cns config partial** { *ip-address* | *hostname* } global configuration command. To cancel a partial configuration, use the **cns config cancel** global configuration command.

Monitoring CNS Configurations

Table 24: CNS show Commands

Command	Purpose
show cns config connections `Switch# show cns config connections`	Displays the status of the CNS Cisco IOS CNS agent connections.
show cns config outstanding `Switch# show cns config outstanding`	Displays information about incremental (partial) CNS configurations that have started but are not yet completed.
show cns config stats `Switch# show cns config stats`	Displays statistics about the Cisco IOS CNS agent.
show cns event connections `Switch# show cns event connections`	Displays the status of the CNS event agent connections.
show cns event gateway `Switch# show cns event gateway`	Displays the event gateway information for your switch.
show cns event stats `Switch# show cns event stats`	Displays statistics about the CNS event agent.
show cns event subject `Switch# show cns event subject`	Displays a list of event agent subjects that are subscribed to by applications.

Additional References

Related Documents

Related Topic	Document Title
Configuration Engine Setup	*Cisco Configuration Engine Installation and Setup Guide, 1.5 for Linux* https://www.cisco.com/en/US/docs/net_mgmt/configuration_engine/1.5/installation_linux/guide/setup_1.html

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
None	-

MIBs

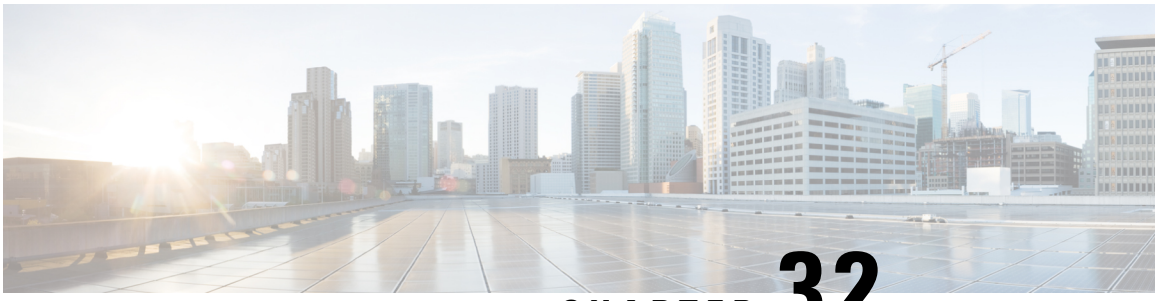
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for the Configuration Engine

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 32

Configuring the Cisco Discovery Protocol

Information About CDP

CDP Overview

CDP is a device discovery protocol that runs over Layer 2 (the data-link layer) on all Cisco-manufactured devices (routers, bridges, access servers, controllers, and switches) and allows network management applications to discover Cisco devices that are neighbors of already known devices. With CDP, network management applications can learn the device type and the Simple Network Management Protocol (SNMP) agent address of neighboring devices running lower-layer, transparent protocols. This feature enables applications to send SNMP queries to neighboring devices.

CDP runs on all media that support Subnetwork Access Protocol (SNAP). Because CDP runs over the data-link layer only, two systems that support different network-layer protocols can learn about each other.

Each CDP-configured device sends periodic messages to a multicast address, advertising at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime information, which is the length of time a receiving device holds CDP information before discarding it. Each device also listens to the messages sent by other devices to learn about neighboring devices.

On the switch, CDP enables Network Assistant to display a graphical view of the network. The switch uses CDP to find cluster candidates and maintain information about cluster members and other devices up to three cluster-enabled devices away from the command switch by default.

CDP and Stacks

A switch stack appears as a single switch in the network. Therefore, CDP discovers the switch stack, not the individual stack members. The switch stack sends CDP messages to neighboring network devices when there are changes to the switch stack membership, such as stack members being added or removed.

Default CDP Configuration

This table shows the default CDP configuration.

Feature	Default Setting
CDP global state	Enabled
CDP interface state	Enabled
CDP timer (packet update frequency)	60 seconds
CDP holdtime (before discarding)	180 seconds
CDP Version-2 advertisements	Enabled

How to Configure CDP

Configuring CDP Characteristics

You can configure these CDP characteristics:

- Frequency of CDP updates
- Amount of time to hold the information before discarding it
- Whether or not to send Version-2 advertisements

Note Steps 3 through 5 are all optional and can be performed in any order.

Follow these steps to configure the CDP characteristics.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose
Step 3	**cdp timer** *seconds* **Example:** `Switch(config)# cdp timer 20`	(Optional) Sets the transmission frequency of CDP updates in seconds. The range is 5 to 254; the default is 60 seconds.
Step 4	**cdp holdtime** *seconds* **Example:** `Switch(config)# cdp holdtime 60`	(Optional) Specifies the amount of time a receiving device should hold the information sent by your device before discarding it. The range is 10 to 255 seconds; the default is 180 seconds.
Step 5	**cdp advertise-v2** **Example:** `Switch(config)# cdp advertise-v2`	(Optional) Configures CDP to send Version-2 advertisements. This is the default state.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

Use the **no** form of the CDP commands to return to the default settings.

Disabling CDP

CDP is enabled by default.

Note Switch clusters and other Cisco devices (such as Cisco IP Phones) regularly exchange CDP messages. Disabling CDP can interrupt cluster discovery and device connectivity.

Follow these steps to disable the CDP device discovery capability.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**no cdp run** **Example:** `Switch(config)# no cdp run`	Disables CDP.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

You must reenable CDP to use it.

Enabling CDP

CDP is enabled by default.

Note Switch clusters and other Cisco devices (such as Cisco IP Phones) regularly exchange CDP messages. Disabling CDP can interrupt cluster discovery and device connectivity.

Follow these steps to enable CDP when it has been disabled.

Before you begin

CDP must be disabled, or it cannot be enabled.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**cdp run** **Example:** `Switch(config)# cdp run`	Enables CDP if it has been disabled.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

Use the **show run all** command to show that CDP has been enabled. If you enter only **show run**, the enabling of CDP may not be displayed.

Disabling CDP on an Interface

CDP is enabled by default on all supported interfaces to send and to receive CDP information.

Note Switch clusters and other Cisco devices (such as Cisco IP Phones) regularly exchange CDP messages. Disabling CDP can interrupt cluster discovery and device connectivity.

Follow these steps to disable CDP on a port.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/1`	Specifies the interface on which you are disabling CDP, and enters interface configuration mode.
Step 4	**no cdp enable** **Example:** `Switch(config-if)# no cdp enable`	Disables CDP on the interface specified in Step 3.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:**	Verifies your entries.

	Command or Action	Purpose
	`Switch# show running-config`	
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Enabling CDP on an Interface

CDP is enabled by default on all supported interfaces to send and to receive CDP information.

Note Switch clusters and other Cisco devices (such as Cisco IP Phones) regularly exchange CDP messages. Disabling CDP can interrupt cluster discovery and device connectivity.

Follow these steps to enable CDP on a port on which it has been disabled.

Before you begin

CDP must be disabled on the port that you are trying to CDP enable on, or it cannot be enabled.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/1`	Specifies the interface on which you are enabling CDP, and enters interface configuration mode.
Step 4	**cdp enable** **Example:**	Enables CDP on a disabled interface.

	Command or Action	Purpose
	`Switch(config-if)# cdp enable`	
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Monitoring and Maintaining CDP

Table 25: Commands for Displaying CDP Information

Command	Description
clear cdp counters	Resets the traffic counters to zero.
clear cdp table	Deletes the CDP table of information about neighbors.
show cdp	Displays global information, such as frequency of transmissions and the holdtime for packets being sent.
show cdp entry *entry-name* [**version**] [**protocol**]	Displays information about a specific neighbor. You can enter an asterisk (*) to display all CDP neighbors, or you can enter the name of the neighbor about which you want information. You can also limit the display to information about the protocols enabled on the specified neighbor or information about the version of software running on the device.
show cdp interface [*interface-id*]	Displays information about interfaces where CDP is enabled. You can limit the display to the interface about which you want information.

Command	Description
show cdp neighbors [*interface-id*] [*detail*]	Displays information about neighbors, including device type, interface type and number, holdtime settings, capabilities, platform, and port ID. You can limit the display to neighbors of a specific interface or expand the display to provide more detailed information.
show cdp traffic	Displays CDP counters, including the number of packets sent and received and checksum errors.

Additional References

Related Documents

Related Topic	Document Title
System Management Commands	*Network Management Command Reference, Cisco IOS XE Release 3E*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
None	-

MIBs

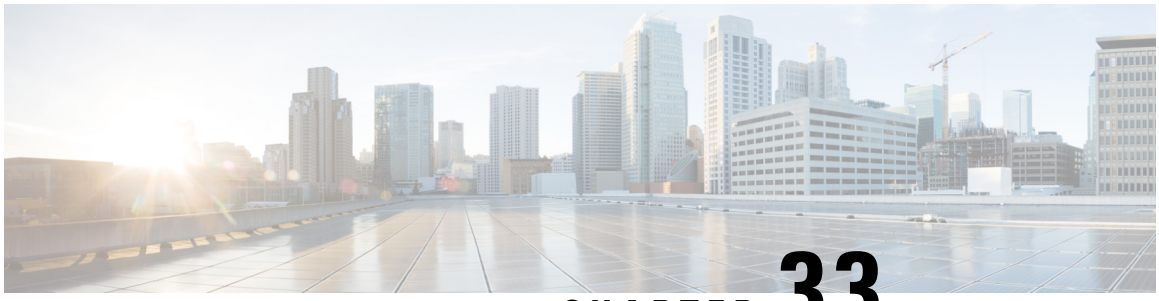
MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for Cisco Discovery Protocol

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 33

Configuring Simple Network Management Protocol

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for SNMP

Supported SNMP Versions

This software release supports the following SNMP versions:

- SNMPv1—The Simple Network Management Protocol, a Full Internet Standard, defined in RFC 1157.
- SNMPv2C replaces the Party-based Administrative and Security Framework of SNMPv2Classic with the community-string-based Administrative Framework of SNMPv2C while retaining the bulk retrieval and improved error handling of SNMPv2Classic. It has these features:

- SNMPv2—Version 2 of the Simple Network Management Protocol, a Draft Internet Standard, defined in RFCs 1902 through 1907.
- SNMPv2C—The community-string-based Administrative Framework for SNMPv2, an Experimental Internet Protocol defined in RFC 1901.

- SNMPv3—Version 3 of the SNMP is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network and includes these security features:
  - Message integrity—Ensures that a packet was not tampered with in transit.
  - Authentication—Determines that the message is from a valid source.
  - Encryption—Mixes the contents of a package to prevent it from being read by an unauthorized source.

Note To select encryption, enter the **priv** keyword.

Both SNMPv1 and SNMPv2C use a community-based form of security. The community of managers able to access the agent's MIB is defined by an IP address access control list and password.

SNMPv2C includes a bulk retrieval function and more detailed error message reporting to management stations. The bulk retrieval function retrieves tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2C improved error-handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes in SNMPv2C report the error type.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy set up for a user and the group within which the user resides. A security level is the permitted level of security within a security model. A combination of the security level and the security model determine which security method is used when handling an SNMP packet. Available security models are SNMPv1, SNMPv2C, and SNMPv3.

The following table identifies characteristics and compares different combinations of security models and levels:

Table 26: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	Result
SNMPv1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv2C	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv3	noAuthNoPriv	Username	No	Uses a username match for authentication.

Model	Level	Authentication	Encryption	Result
SNMPv3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
SNMPv3	authPriv	MD5 or SHA	Data Encryption Standard (DES) or Advanced Encryption Standard (AES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allows specifying the User-based Security Model (USM) with these encryption algorithms: • DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard. • 3DES 168-bit encryption • AES 128-bit, 192-bit, or 256-bit encryption

You must configure the SNMP agent to use the SNMP version supported by the management station. Because an agent can communicate with multiple managers, you can configure the software to support communications using SNMPv1, SNMPv2C, or SNMPv3.

Restrictions for SNMP

Version Restrictions

- SNMPv1 does not support informs.

Information About SNMP

SNMP Overview

SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a management information base (MIB). The SNMP manager can be part of a network management system (NMS) such as Cisco Prime Infrastructure. The agent and MIB reside on the switch. To configure SNMP on the switch, you define the relationship between the manager and the agent.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data.

An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can mean improper user authentication, restarts, link status (up or down), MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events.

SNMP Manager Functions

The SNMP manager uses information in the MIB to perform the operations described in the following table:

Table 27: SNMP Operations

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves a value from a variable within a table.[3]
get-bulk-request[4]	Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data.
get-response	Replies to a get-request, get-next-request, and set-request sent by an NMS.
set-request	Stores a value in a specific variable.
trap	An unsolicited message sent by an SNMP agent to an SNMP manager when some event has occurred.

[3] With this operation, an SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.

[4] The get-bulk command only works with SNMPv2 or later.

SNMP Agent Functions

The SNMP agent responds to SNMP manager requests as follows:

- Get a MIB variable—The SNMP agent begins this function in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.

- Set a MIB variable—The SNMP agent begins this function in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

The SNMP agent also sends unsolicited trap messages to notify an NMS that a significant event has occurred on the agent. Examples of trap conditions include, but are not limited to, when a port or module goes up or down, when spanning-tree topology changes occur, and when authentication failures occur.

Related Topics

Disabling the SNMP Agent, on page 439
Monitoring SNMP Status, on page 456

SNMP Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the NMS to access the switch, the community string definitions on the NMS must match at least one of the three community string definitions on the switch.

A community string can have one of the following attributes:

- Read-only (RO)—Gives all objects in the MIB except the community strings read access to authorized management stations, but does not allow write access.
- Read-write (RW)—Gives all objects in the MIB read and write access to authorized management stations, but does not allow access to the community strings.
- When a cluster is created, the command switch manages the exchange of messages among member switches and the SNMP application. The Network Assistant software appends the member switch number (@esN, where N is the switch number) to the first configured RW and RO community strings on the command switch and propagates them to the member switches.

Related Topics

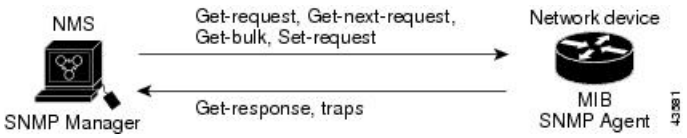
Configuring Community Strings, on page 441

SNMP MIB Variables Access

An example of an NMS is the Cisco Prime Infrastructure network management software. Cisco Prime Infrastructure 2.0 software uses the switch MIB variables to set device variables and to poll devices on the network for specific information. The results of a poll can be displayed as a graph and analyzed to troubleshoot internetworking problems, increase network performance, verify the configuration of devices, monitor traffic loads, and more.

As shown in the figure, the SNMP agent gathers data from the MIB. The agent can send traps, or notification of certain events, to the SNMP manager, which receives and processes the traps. Traps alert the SNMP manager to a condition on the network such as improper user authentication, restarts, link status (up or down), MAC address tracking, and so forth. The SNMP agent also responds to MIB-related queries sent by the SNMP manager in *get-request*, *get-next-request*, and *set-request* format.

Figure 31: SNMP Network



SNMP Notifications

SNMP allows the switch to send notifications to SNMP managers when particular events occur. SNMP notifications can be sent as traps or inform requests. In command syntax, unless there is an option in the command to select either traps or informs, the keyword traps refers to either traps or informs, or both. Use the **snmp-server host** command to specify whether to send SNMP notifications as traps or informs.

Note SNMPv1 does not support informs.

Traps are unreliable because the receiver does not send an acknowledgment when it receives a trap, and the sender cannot determine if the trap was received. When an SNMP manager receives an inform request, it acknowledges the message with an SNMP response protocol data unit (PDU). If the sender does not receive a response, the inform request can be sent again. Because they can be resent, informs are more likely than traps to reach their intended destination.

The characteristics that make informs more reliable than traps also consume more resources in the switch and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request is held in memory until a response is received or the request times out. Traps are sent only once, but an inform might be resent or retried several times. The retries increase traffic and contribute to a higher overhead on the network. Therefore, traps and informs require a trade-off between reliability and resources. If it is important that the SNMP manager receive every notification, use inform requests. If traffic on the network or memory in the switch is a concern and notification is not required, use traps.

Related Topics

Configuring SNMP Notifications, on page 446
Monitoring SNMP Status, on page 456

SNMP ifIndex MIB Object Values

The SNMP agent's IF-MIB module comes up shortly after reboot. As various physical interface drivers are initialized they register with the IF-MIB module, essentially saying "Give me an ifIndex number". The IF-MIB module assigns the next available ifIndex number on a first-come-first-served basis. That is, minor differences in driver initialization order from one reboot to another can result in the same physical interface getting a different ifIndex number than it had before the reboot (unless ifIndex persistency is enabled of course).

Default SNMP Configuration

Feature	Default Setting
SNMP agent	Disabled[5].
SNMP trap receiver	None configured.
SNMP traps	None enabled except the trap for TCP connections (tty).
SNMP version	If no version keyword is present, the default is Version 1.
SNMPv3 authentication	If no keyword is entered, the default is the **noauth** (noAuthNoPriv) security level.
SNMP notification type	If no type is specified, all notifications are sent.

[5] This is the default when the switch starts and the startup configuration does not have any **snmp-server** global configuration commands.

SNMP Configuration Guidelines

If the switch starts and the switch startup configuration has at least one **snmp-server** global configuration command, the SNMP agent is enabled.

An SNMP *group* is a table that maps SNMP users to SNMP views. An SNMP *user* is a member of an SNMP group. An SNMP *host* is the recipient of an SNMP trap operation. An SNMP *engine ID* is a name for the local or remote SNMP engine.

When configuring SNMP, follow these guidelines:

- When configuring an SNMP group, do not specify a notify view. The **snmp-server host** global configuration command auto-generates a notify view for the user and then adds it to the group associated with that user. Modifying the group's notify view affects all users associated with that group.
- To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides.
- Before you configure remote users for a particular agent, configure the SNMP engine ID, using the **snmp-server engineID** global configuration command with the **remote** option. The remote agent's SNMP engine ID and user password are used to compute the authentication and privacy digests. If you do not configure the remote engine ID first, the configuration command fails.
- When configuring SNMP informs, you need to configure the SNMP engine ID for the remote agent in the SNMP database before you can send proxy requests or informs to it.
- If a local user is not associated with a remote host, the switch does not send informs for the **auth** (authNoPriv) and the **priv** (authPriv) authentication levels.
- Changing the value of the SNMP engine ID has significant results. A user's password (entered on the command line) is converted to an MD5 or SHA security digest based on the password and the local engine ID. The command-line password is then destroyed, as required by RFC 2274. Because of this deletion, if the value of the engine ID changes, the security digests of SNMPv3 users become invalid, and you need to reconfigure SNMP users by using the **snmp-server user** *username* global configuration command. Similar restrictions require the reconfiguration of community strings when the engine ID changes.

Related Topics

Configuring SNMP Groups and Users, on page 443
Monitoring SNMP Status, on page 456

How to Configure SNMP

Disabling the SNMP Agent

The **no snmp-server** global configuration command disables all running versions (Version 1, Version 2C, and Version 3) of the SNMP agent on the device. You reenable all versions of the SNMP agent by the first

snmp-server global configuration command that you enter. There is no Cisco IOS command specifically designated for enabling SNMP.

Follow these steps to disable the SNMP agent.

Before you begin

The SNMP Agent must be enabled before it can be disabled. The SNMP agent is enabled by the first **snmp-server** global configuration command entered on the device.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**no snmp-server** **Example:** `Switch(config)# no snmp-server`	Disables the SNMP agent operation.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

SNMP Agent Functions, on page 436
Monitoring SNMP Status, on page 456

Configuring Community Strings

You use the SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the switch. Optionally, you can specify one or more of these characteristics associated with the string:

- An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent
- A MIB view, which defines the subset of all MIB objects accessible to the given community
- Read and write or read-only permission for the MIB objects accessible to the community

Follow these steps to configure a community string on the switch.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [*access-list-number*] **Example:** `Switch(config)# snmp-server community comaccess ro 4`	Configures the community string. **Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command. • For *string*, specify a string that acts like a password and permits access to the SNMP protocol. You can configure one or more community strings of any length. • (Optional) For **view**, specify the view record accessible to the community. • (Optional) Specify either read-only (**ro**) if you want authorized management stations to retrieve MIB objects, or specify

	Command or Action	Purpose
		read-write (**rw**) if you want authorized management stations to retrieve and modify MIB objects. By default, the community string permits read-only access to all objects. • (Optional) For *access-list-number*, enter an IP standard access list numbered from 1 to 99 and 1300 to 1999.
Step 4	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] **Example:** `Switch(config)# access-list 4 deny any`	(Optional) If you specified an IP standard access list number in Step 3, then create the list, repeating the command as many times as necessary. • For *access-list-number*, enter the access list number specified in Step 3. • The **deny** keyword denies access if the conditions are matched. The **permit** keyword permits access if the conditions are matched. • For *source*, enter the IP address of the SNMP managers that are permitted to use the community string to gain access to the agent. • (Optional) For *source-wildcard*, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore. Recall that the access list is always terminated by an implicit deny statement for everything.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:**	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	`Switch# copy running-config startup-config`	

What to do next

To disable access for an SNMP community, set the community string for that community to the null string (do not enter a value for the community string).

To remove a specific community string, use the **no snmp-server** community string global configuration command.

You can specify an identification name (engine ID) for the local or remote SNMP server engine on the switch. You can configure an SNMP server group that maps SNMP users to SNMP views, and you can add new users to the SNMP group.

Related Topics

SNMP Community Strings, on page 437

Configuring SNMP Groups and Users

You can specify an identification name (engine ID) for the local or remote SNMP server engine on the switch. You can configure an SNMP server group that maps SNMP users to SNMP views, and you can add new users to the SNMP group.

Follow these steps to configure SNMP groups and users on the switch.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**snmp-server engineID** {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*} **Example:** `Switch(config)# snmp-server engineID local 1234`	Configures a name for either the local or remote copy of SNMP. • The *engineid-string* is a 24-character ID string with the name of the copy of SNMP. You need not specify the entire 24-character engine ID if it has trailing zeros. Specify only the portion of the

	Command or Action	Purpose
		engine ID up to the point where only zeros remain in the value. The Step Example configures an engine ID of 123400000000000000000000. • If you select **remote**, specify the *ip-address* of the device that contains the remote copy of SNMP and the optional User Datagram Protocol (UDP) port on the remote device. The default is 162.
Step 4	**snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*] **Example:** `Switch(config)# snmp-server group public v2c access lmnop`	Configures a new SNMP group on the remote device. For *group-name*, specify the name of the group. Specify one of the following security models: • **v1** is the least secure of the possible security models. • **v2c** is the second least secure model. It allows transmission of informs and integers twice the normal width. • **v3**, the most secure, requires you to select one of the following authentication levels: **auth**—Enables the Message Digest 5 (MD5) and the Secure Hash Algorithm (SHA) packet authentication. **noauth**—Enables the noAuthNoPriv security level. This is the default if no keyword is specified. **priv**—Enables Data Encryption Standard (DES) packet encryption (also called privacy). (Optional) Enter **read** *readview* with a string (not to exceed 64 characters) that is the name of the view in which you can only view the contents of the agent. (Optional) Enter **write** *writeview* with a string (not to exceed 64 characters) that is the name of the view in which you enter data and configure the contents of the agent. (Optional) Enter **notify** *notifyview* with a string (not to exceed 64 characters) that is the name of the view in which you specify a notify, inform, or trap.

	Command or Action	Purpose
		(Optional) Enter **access** *access-list* with a string (not to exceed 64 characters) that is the name of the access list.
Step 5	**snmp-server user** *username group-name* {**remote** *host* [**udp-port** *port*] } {**v1** [**access** *access-list*] | **v2c** [**access** *access-list*] | **v3** [**encrypted**] [**access** *access-list*] [**auth** {**md5** | **sha**} *auth-password*] } [*priv* {**des** | **3des** | **aes** {**128** | **192** | **256**} } *priv-password*] **Example:** `Switch(config)# snmp-server user Pat public v2c`	Adds a new user for an SNMP group. The *username* is the name of the user on the host that connects to the agent. The *group-name* is the name of the group to which the user is associated. Enter **remote** to specify a remote SNMP entity to which the user belongs and the hostname or IP address of that entity with the optional UDP port number. The default is 162. Enter the SNMP version number (**v1**, **v2c**, or **v3**). If you enter **v3**, you have these additional options: • **encrypted** specifies that the password appears in encrypted format. This keyword is available only when the **v3** keyword is specified. • **auth** is an authentication level setting session that can be either the HMAC-MD5-96 (**md5**) or the HMAC-SHA-96 (**sha**) authentication level and requires a password string *auth-password* (not to exceed 64 characters). If you enter **v3** you can also configure a private (**priv**) encryption algorithm and password string *priv-password* using the following keywords (not to exceed 64 characters): • **priv** specifies the User-based Security Model (USM). • **des** specifies the use of the 56-bit DES algorithm. • **3des** specifies the use of the 168-bit DES algorithm. • **aes** specifies the use of the DES algorithm. You must select either 128-bit, 192-bit, or 256-bit encryption.

	Command or Action	Purpose
		(Optional) Enter **access** *access-list* with a string (not to exceed 64 characters) that is the name of the access list.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

SNMP Configuration Guidelines, on page 439
Monitoring SNMP Status, on page 456

Configuring SNMP Notifications

A trap manager is a management station that receives and processes traps. Traps are system alerts that the switch generates when certain events occur. By default, no trap manager is defined, and no traps are sent. Switches running this Cisco IOS release can have an unlimited number of trap managers.

Note Many commands use the word **traps** in the command syntax. Unless there is an option in the command to select either traps or informs, the keyword **traps** refers to traps, informs, or both. Use the **snmp-server host** global configuration command to specify whether to send SNMP notifications as traps or informs.

You can use the **snmp-server host** global configuration command for a specific host to receive the notification types listed in the following table. You can enable any or all of these traps and configure a trap manager to receive them.

Table 28: Device Notification Types

Notification Type Keyword	Description
bridge	Generates STP bridge MIB traps.
cluster	Generates a trap when the cluster configuration changes.

Notification Type Keyword	Description
config	Generates a trap for SNMP configuration changes.
copy-config	Generates a trap for SNMP copy configuration changes.
cpu threshold	Allow CPU-related traps.
entity	Generates a trap for SNMP entity changes.
envmon	Generates environmental monitor traps. You can enable any or all of these environmental traps: fan, shutdown, status, supply, temperature.
flash	Generates SNMP FLASH notifications. In a switch stack, you can optionally enable notification for flash insertion or removal, which would cause a trap to be issued whenever a switch in the stack is removed or inserted (physical removal, power cycle, or reload).
fru-ctrl	Generates entity field-replaceable unit (FRU) control traps. In the switch stack, this trap refers to the insertion or removal of a switch in the stack.
hsrp	Generates a trap for Hot Standby Router Protocol (HSRP) changes.
ipmulticast	Generates a trap for IP multicast routing changes.
mac-notification	Generates a trap for MAC address notifications.
ospf	Generates a trap for Open Shortest Path First (OSPF) changes. You can enable any or all of these traps: Cisco specific, errors, link-state advertisement, rate limit, retransmit, and state changes.
pim	Generates a trap for Protocol-Independent Multicast (PIM) changes. You can enable any or all of these traps: invalid PIM messages, neighbor changes, and rendezvous point (RP)-mapping changes.
port-security	Generates SNMP port security traps. You can also set a maximum trap rate per second. The range is from 0 to 1000; the default is 0, which means that there is no rate limit. **Note** When you configure a trap by using the notification type **port-security**, configure the port security trap first, and then configure the port security trap rate: **1. snmp-server enable traps port-security** **2. snmp-server enable traps port-security trap-rate** *rate*
snmp	Generates a trap for SNMP-type notifications for authentication, cold start, warm start, link up or link down.
storm-control	Generates a trap for SNMP storm-control. You can also set a maximum trap rate per minute. The range is from 0 to 1000; the default is 0 (no limit is imposed; a trap is sent at every occurrence).
stpx	Generates SNMP STP Extended MIB traps.
syslog	Generates SNMP syslog traps.

Notification Type Keyword	Description
tty	Generates a trap for TCP connections. This trap is enabled by default.
vlan-membership	Generates a trap for SNMP VLAN membership changes.
vlancreate	Generates SNMP VLAN created traps.
vlandelete	Generates SNMP VLAN deleted traps.
vtp	Generates a trap for VLAN Trunking Protocol (VTP) changes.

Follow these steps to configure the switch to send traps or informs to a host.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**snmp-server engineID remote** *ip-address engineid-string* **Example:** `Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b`	Specifies the engine ID for the remote host.
Step 4	**snmp-server user** *username group-name* {**remote** *host* [**udp-port** *port*] } {**v1** [**access** *access-list*] | **v2c** [**access** *access-list*] | **v3** [**encrypted**] [**access** *access-list*] [**auth** {**md5** | **sha**} *auth-password*] } **Example:** `Switch(config)# snmp-server user Pat public v2c`	Configures an SNMP user to be associated with the remote host created in Step 3. **Note** You cannot configure a remote user for an address without first configuring the engine ID for the remote host. Otherwise, you receive an error message, and the command is not executed.
Step 5	**snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*] **Example:** `Switch(config)# snmp-server group public v2c access lmnop`	Configures an SNMP group.

	Command or Action	Purpose
Step 6	**snmp-server host** *host-addr* [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}] *community-string* [*notification-type*] **Example:** `Switch(config)# snmp-server host 203.0.113.1 comaccess snmp`	Specifies the recipient of an SNMP trap operation. For *host-addr*, specify the name or Internet address of the host (the targeted recipient). (Optional) Specify **traps** (the default) to send SNMP traps to the host. (Optional) Specify **informs** to send SNMP informs to the host. (Optional) Specify the SNMP **version** (**1**, **2c**, or **3**). SNMPv1 does not support informs. (Optional) For Version 3, select authentication level **auth**, **noauth**, or **priv**. **Note** The **priv** keyword is available only when the cryptographic software image is installed. For *community-string*, when **version 1** or **version 2c** is specified, enter the password-like community string sent with the notification operation. When **version 3** is specified, enter the SNMPv3 username. The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command. (Optional) For *notification-type*, use the keywords listed in the table above. If no type is specified, all notifications are sent. **Note** In case of SNMP version 3, SNMPv3 user should be configured prior SNMPv3 host configuration, otherwise SNMP traps will not be sent.
Step 7	**snmp-server enable traps** *notification-types* **Example:** `Switch(config)# snmp-server enable traps snmp`	Enables the switch to send traps or informs and specifies the type of notifications to be sent. For a list of notification types, see the table above, or enter **snmp-server enable traps ?** To enable multiple types of traps, you must enter a separate **snmp-server enable traps** command for each trap type.

	Command or Action	Purpose
		Note When you configure a trap by using the notification type **port-security**, configure the port security trap first, and then configure the port security trap rate: 1. **snmp-server enable traps port-security** 2. **snmp-server enable traps port-security trap-rate** *rate*
Step 8	**snmp-server trap-source** *interface-id* **Example:** `Switch(config)# snmp-server trap-source GigabitEthernet1/0/1`	(Optional) Specifies the source interface, which provides the IP address for the trap message. This command also sets the source IP address for informs.
Step 9	**snmp-server queue-length** *length* **Example:** `Switch(config)# snmp-server queue-length 20`	(Optional) Establishes the message queue length for each trap host. The range is 1 to 5000; the default is 10.
Step 10	**snmp-server trap-timeout** *seconds* **Example:** `Switch(config)# snmp-server trap-timeout 60`	(Optional) Defines how often to resend trap messages. The range is 1 to 1000; the default is 30 seconds.
Step 11	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 12	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 13	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

The **snmp-server host** command specifies which hosts receive the notifications. The **snmp-server enable traps** command globally enables the method for the specified notification (for traps and informs). To enable a host to receive an inform, you must configure an **snmp-server host informs** command for the host and globally enable informs by using the **snmp-server enable traps** command.

To remove the specified host from receiving traps, use the **no snmp-server host** *host* global configuration command. The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** global configuration command. To disable a specific trap type, use the **no snmp-server enable traps** *notification-types* global configuration command.

Related Topics

SNMP Notifications, on page 438
Monitoring SNMP Status, on page 456

Setting the Agent Contact and Location Information

Follow these steps to set the system contact and location of the SNMP agent so that these descriptions can be accessed through the configuration file.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**snmp-server contact** *text* **Example:** `Switch(config)# snmp-server contact Dial System Operator at beeper 21555`	Sets the system contact string.
Step 4	**snmp-server location** *text* **Example:** `Switch(config)# snmp-server location Building 3/Room 222`	Sets the system location string.
Step 5	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Switch(config)# end`	
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Limiting TFTP Servers Used Through SNMP

Follow these steps to limit the TFTP servers used for saving and loading configuration files through SNMP to the servers specified in an access list.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**snmp-server tftp-server-list** *access-list-number* **Example:** `Switch(config)# snmp-server tftp-server-list 44`	Limits the TFTP servers used for configuration file copies through SNMP to the servers in the access list. For *access-list-number*, enter an IP standard access list numbered from 1 to 99 and 1300 to 1999.
Step 4	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] **Example:**	Creates a standard access list, repeating the command as many times as necessary. For *access-list-number*, enter the access list number specified in Step 3.

	Command or Action	Purpose
	`Switch(config)# access-list 44 permit 10.1.1.2`	The **deny** keyword denies access if the conditions are matched. The **permit** keyword permits access if the conditions are matched. For *source*, enter the IP address of the TFTP servers that can access the switch. (Optional) For *source-wildcard*, enter the wildcard bits, in dotted decimal notation, to be applied to the source. Place ones in the bit positions that you want to ignore. The access list is always terminated by an implicit deny statement for everything.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Trap Flags for SNMP

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose
Step 2	**trapflags ap** { **interfaceup** | **register**} **Example:** `Switch(config)# trapflags ap interfaceup`	Enables sending AP-related traps. Use the **no** form of the command to disable the trap flags. • **interfaceup**– Enables trap when a Cisco AP interface (A or B) comes up. • **register**– Enables trap when a Cisco AP registers with a Cisco switch.
Step 3	**trapflags client** {**dot11** | **excluded**} **Example:** `Switch(config)# trapflags client excluded`	Enables sending client-related dot11 traps. Use the **no** form of the command to disable the trap flags. • **dot11**– Enables Dot11 traps for clients. • **excluded**– Enables excluded traps for clients.
Step 4	**trapflags dot11-security** {**ids-sig-attack** | **wep-decrypt-error**} **Example:** `Switch(config)# trapflags dot11-security wep-decrypt-error`	Enables sending 802.11 security-related traps. Use the **no** form of the command to disable the trap flags. • **ids-sig-attack**– Enables IDS signature attack traps. • **wep-decrypt-error**– Enables traps for WEP decrypt error for clients.
Step 5	**trapflags mesh** **Example:** `Switch(config)# trapflags mesh`	Enables trap for the mesh. Use the **no** form of the command to disable the trap flags.
Step 6	**trapflags rogueap** **Example:** `Switch(config)# trapflags rogueap`	Enables trap for rogue AP detection. Use the **no** form of the command to disable the trap flags.
Step 7	**trapflags rrm-params** {**channels** | **tx-power**} **Example:** `Switch(config)# trapflags rrm-params tx-power`	Enables sending RRM-parameter update-related traps. Use the **no** form of the command to disable the trap flags. • **channels**– Enables trap when RF Manager automatically changes a channel number for the Cisco AP interface. • **tx-power**– Enables the trap when RF Manager automatically changes Tx-Power level for the Cisco AP interface.

	Command or Action	Purpose
Step 8	**trapflags rrm-profile** {**coverage** | **interference** | **load** | **noise**} **Example:** `Switch(config)# trapflags rrm-profile interference`	Enables sending RRM-profile-related traps. Use the **no** form of the command to disable the trap flags. • **coverage**– Enables the trap when the coverage profile maintained by RF Manager fails. • **interference**– Enables the trap when the interference profile maintained by RF Manager fails. • **load**– Enables trap when the load profile maintained by RF Manager fails. • **noise**– Enables trap when the noise profile maintained by RF Manager fails.
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Enabling SNMP Wireless Trap Notification

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**snmp-server enable traps wireless** [**AP** | **RRM** | **bsn80211SecurityTrap** | **bsnAPParamUpdate** | **bsnAPProfile** | **bsnAccessPoint** | **bsnMobileStation** | **bsnRogue** | **client** | **mfp** | **rogue**] **Example:** `Switch(config)# snmp-server enable traps wireless AP`	Enables SNMP wireless trap notification. • **AP**– Enables access point traps. • **RRM**– Enables RRM traps. • **bsn80211SecurityTrap**– Enables the security-related trap. • **bsnAPParamUpdate**– Enables the trap for AP parameters that get updated. • **bsnAPProfile**– Enables BSN AP profile traps.

	Command or Action	Purpose
		• **bsnAccessPoint**– Enables BSN access point traps. • **bsnMobileStation**– Controls wireless client traps. • **bsnRogue**– Enables BSN rogue-related traps. • **client**– Enables client traps. • **mfp**– Enables MFP traps. • **rogue**– Enables rogue-related traps.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Monitoring SNMP Status

To display SNMP input and output statistics, including the number of illegal community string entries, errors, and requested variables, use the **show snmp** privileged EXEC command. You also can use the other privileged EXEC commands listed in the table to display SNMP information.

Table 29: Commands for Displaying SNMP Information

Command	Purpose
show snmp	Displays SNMP statistics.
show snmp engineID	Displays information on the local SNMP engine and all remote engines that have been configured on the device.
show snmp group	Displays information on each SNMP group on the network.
show snmp pending	Displays information on pending SNMP requests.
show snmp sessions	Displays information on the current SNMP sessions.

Command	Purpose
show snmp user	Displays information on each SNMP user name in the SNMP users table. **Note** You must use this command to display SNMPv3 configuration information for **auth** | **noauth** | **priv** mode. This information is not displayed in the **show running-config** output.

Related Topics

Disabling the SNMP Agent, on page 439
SNMP Agent Functions, on page 436
Configuring SNMP Groups and Users, on page 443
SNMP Configuration Guidelines, on page 439
Configuring SNMP Notifications, on page 446
SNMP Notifications, on page 438

SNMP Examples

This example shows how to enable all versions of SNMP. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string *public*. This configuration does not cause the switch to send any traps.

```
Switch(config)# snmp-server community public
```

This example shows how to permit any SNMP manager to access all objects with read-only permission using the community string *public*. The switch also sends VTP traps to the hosts 192.180.1.111 and 192.180.1.33 using SNMPv1 and to the host 192.180.1.27 using SNMPv2C. The community string *public* is sent with the traps.

```
Switch(config)# snmp-server community public
Switch(config)# snmp-server enable traps vtp
Switch(config)# snmp-server host 192.180.1.27 version 2c public
Switch(config)# snmp-server host 192.180.1.111 version 1 public
Switch(config)# snmp-server host 192.180.1.33 public
```

This example shows how to allow read-only access for all objects to members of access list 4 that use the *comaccess* community string. No other SNMP managers have access to any objects. SNMP Authentication Failure traps are sent by SNMPv2C to the host *cisco.com* using the community string *public*.

```
Switch(config)# snmp-server community comaccess ro 4
Switch(config)# snmp-server enable traps snmp authentication
Switch(config)# snmp-server host cisco.com version 2c public
```

This example shows how to send Entity MIB traps to the host *cisco.com*. The community string is restricted. The first line enables the switch to send Entity MIB traps in addition to any traps previously enabled. The second line specifies the destination of these traps and overwrites any previous **snmp-server** host commands for the host *cisco.com*.

```
Switch(config)# snmp-server enable traps entity
Switch(config)# snmp-server host cisco.com restricted entity
```

This example shows how to enable the switch to send all traps to the host *myhost.cisco.com* using the community string *public*:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

This example shows how to associate a user with a remote host and to send **auth** (authNoPriv) authentication-level informs when the user enters global configuration mode:

```
Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
Switch(config)# snmp-server group authgroup v3 auth
Switch(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5 mypassword
Switch(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
Switch(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server inform retries 0
```

Additional References

Related Documents

Related Topic	Document Title
SNMP Commands	*Network Management Command Reference, Cisco IOS XE Release 3E*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
None	-

MIBs

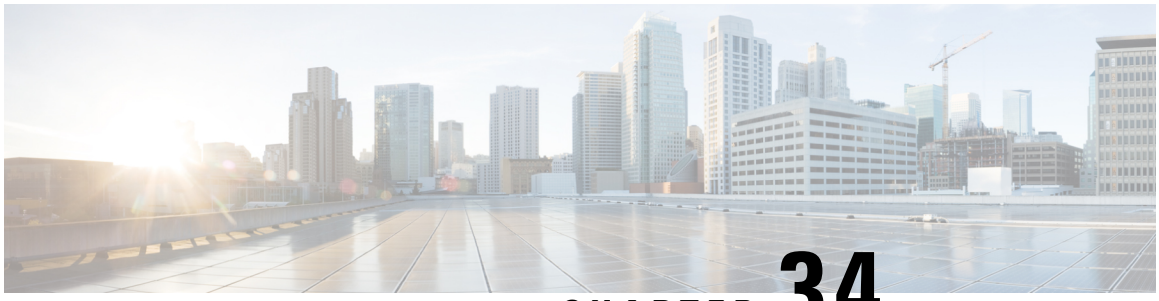
MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for Simple Network Management Protocol

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 34

Configuring Service Level Agreements

This chapter describes how to use Cisco IOS IP Service Level Agreements (SLAs) on the switch.

Unless otherwise noted, the term *switch* refers to a standalone switch or a switch stack.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions on SLAs

This section lists the restrictions on SLAs.

The following are restrictions on IP SLAs network performance measurement:

- The switch does not support VoIP service levels using the gatekeeper registration delay operations measurements.
- Only a Cisco IOS device can be a source for a destination IP SLAs responder.
- You cannot configure the IP SLAs responder on non-Cisco devices and Cisco IOS IP SLAs can send operational packets only to services native to those devices.

Related Topics

Implementing IP SLA Network Performance Measurement, on page 469
Network Performance Measurement with Cisco IOS IP SLAs, on page 463
IP SLA Responder and IP SLA Control Protocol, on page 464

Information About SLAs

Cisco IOS IP Service Level Agreements (SLAs)

Cisco IOS IP SLAs send data across the network to measure performance between multiple network locations or across multiple network paths. They simulate network data and IP services and collect network performance information in real time. Cisco IOS IP SLAs generate and analyze traffic either between Cisco IOS devices or from a Cisco IOS device to a remote IP device such as a network application server. Measurements provided by the various Cisco IOS IP SLA operations can be used for troubleshooting, for problem analysis, and for designing network topologies.

Depending on the specific Cisco IOS IP SLA operations, various network performance statistics are monitored within the Cisco device and stored in both command-line interface (CLI) and Simple Network Management Protocol (SNMP) MIBs. IP SLA packets have configurable IP and application layer options such as source and destination IP address, User Datagram Protocol (UDP)/TCP port numbers, a type of service (ToS) byte (including Differentiated Services Code Point [DSCP] and IP Prefix bits), Virtual Private Network (VPN) routing/forwarding instance (VRF), and URL web address.

Because Cisco IP SLAs are Layer 2 transport independent, you can configure end-to-end operations over disparate networks to best reflect the metrics that an end user is likely to experience. IP SLAs support the use of Cisco Mediatrace and Cisco Performance Monitor to collect and analyze the following performance metrics:

- Delay (both round-trip and one-way)
- Jitter (directional)
- Packet loss (directional)
- Packet sequencing (packet ordering)
- Path (per hop)
- Connectivity (directional)
- Server or website download time

Additionally, the switch also supports Cisco Medianet to enable intelligent services in the network infrastructure for a wide variety of video applications. Cisco Medianet supports the auto-provisioning of endpoints offering video conferencing services and of IP Surveillance cameras through Auto Smartports.

Cisco Mediatrace and Cisco Performance Monitor can be used on switches running the IP Base image or the IP Services image.

Because Cisco IOS IP SLAs is SNMP-accessible, it can also be used by performance-monitoring applications like Cisco Prime Internetwork Performance Monitor (IPM) and other third-party Cisco partner performance management products.

Using IP SLAs can provide the following benefits:

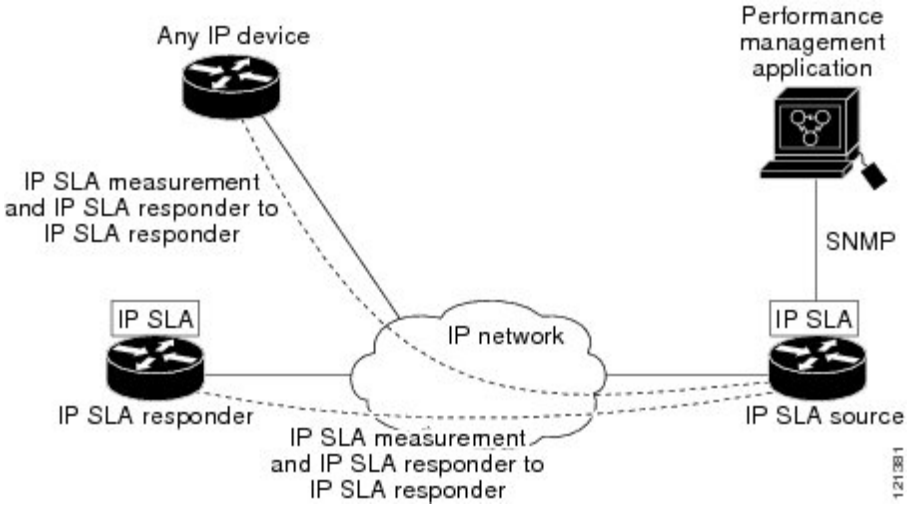
- Service-level agreement monitoring, measurement, and verification.
- Network performance monitoring
  - Measurement of jitter, latency, or packet loss in the network.
  - Continuous, reliable, and predictable measurements.
- IP service network health assessment to verify that the existing QoS is sufficient for new IP services.
- Edge-to-edge network availability monitoring for proactive verification and connectivity testing of network resources (for example, shows the network availability of an NFS server used to store business critical data from a remote site).
- Network operation troubleshooting by providing consistent, reliable measurement that immediately identifies problems and saves troubleshooting time.
- Multiprotocol Label Switching (MPLS) performance monitoring and network verification (if the switch supports MPLS).

Network Performance Measurement with Cisco IOS IP SLAs

You can use IP SLAs to monitor the performance between any area in the network—core, distribution, and edge—without deploying a physical probe. It uses generated traffic to measure network performance between two networking devices.

Figure 32: Cisco IOS IP SLAs Operation

The following figure shows how IP SLAs begin when the source device sends a generated packet to the destination device. After the destination device receives the packet, depending on the type of IP SLAs operation, it responds with time-stamp information for the source to make the calculation on performance metrics. An IP SLAs operation performs a network measurement from the source device to a destination in the network using a specific protocol such as UDP.



Related Topics

Implementing IP SLA Network Performance Measurement, on page 469
Restrictions on SLAs, on page 461

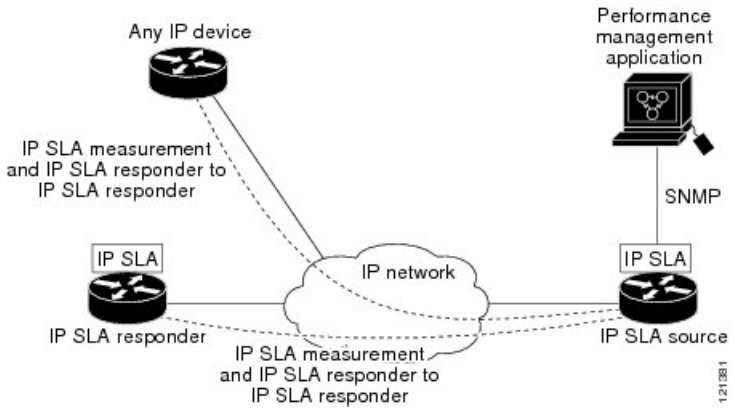
IP SLA Responder and IP SLA Control Protocol

The IP SLA responder is a component embedded in the destination Cisco device that allows the system to anticipate and respond to IP SLA request packets. The responder provides accurate measurements without the need for dedicated probes. The responder uses the Cisco IOS IP SLA Control Protocol to provide a mechanism through which it can be notified on which port it should listen and respond.

Note The IP SLA responder can be a Cisco IOS Layer 2, responder-configurable switch. The responder does not need to support full IP SLA functionality.

The following figure shows where the Cisco IOS IP SLA responder fits in the IP network. The responder listens on a specific port for control protocol messages sent by an IP SLA operation. Upon receipt of the control message, it enables the specified UDP or TCP port for the specified duration. During this time, the responder accepts the requests and responds to them. It disables the port after it responds to the IP SLA packet, or when the specified time expires. MD5 authentication for control messages is available for added security.

Figure 33: Cisco IOS IP SLAs Operation



You do not need to enable the responder on the destination device for all IP SLA operations. For example, a responder is not required for services that are already provided by the destination router (such as Telnet or HTTP).

Related Topics

Restrictions on SLAs, on page 461

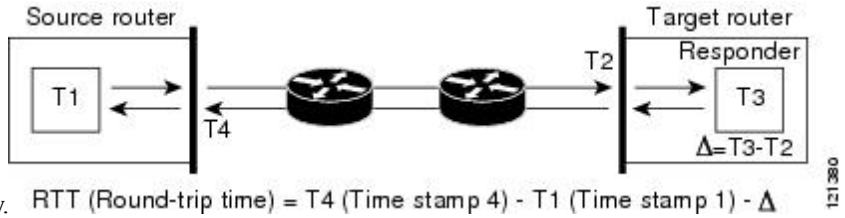
Response Time Computation for IP SLAs

Switches, controllers, and routers can take tens of milliseconds to process incoming packets due to other high priority processes. This delay affects the response times because the test-packet reply might be in a queue while waiting to be processed. In this situation, the response times would not accurately represent true network delays. IP SLAs minimize these processing delays on the source device as well as on the target device (if the responder is being used) to determine true round-trip times. IP SLA test packets use time stamping to minimize the processing delays.

When the IP SLA responder is enabled, it allows the target device to take time stamps when the packet arrives on the interface at interrupt level and again just as it is leaving, eliminating the processing time. This time stamping is made with a granularity of sub-milliseconds (ms).

Figure 34: Cisco IOS IP SLA Responder Time Stamping

The following figure demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target router, with the responder functionality enabled, time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source router where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy.



An additional benefit of the two time stamps at the target device is the ability to track one-way delay, jitter, and directional packet loss. Because much network behavior is asynchronous, it is critical to have these statistics. However, to capture one-way delay measurements, you must configure both the source router and target router with Network Time Protocol (NTP) so that the source and target are synchronized to the same clock source. One-way jitter measurements do not require clock synchronization.

IP SLAs Operation Scheduling

When you configure an IP SLAs operation, you must schedule the operation to begin capturing statistics and collecting error information. You can schedule an operation to start immediately or to start at a certain month, day, and hour. You can use the *pending* option to set the operation to start at a later time. The pending option is an internal state of the operation that is visible through SNMP. The pending state is also used when an operation is a reaction (threshold) operation waiting to be triggered. You can schedule a single IP SLAs operation or a group of operations at one time.

You can schedule several IP SLAs operations by using a single command through the Cisco IOS CLI or the CISCO RTTMON-MIB. Scheduling the operations to run at evenly distributed times allows you to control the amount of IP SLAs monitoring traffic. This distribution of IP SLA operations helps minimize the CPU utilization and thus improves network scalability.

For more details about the IP SLA multi-operations scheduling functionality, see the “IP SLAs—Multiple Operation Scheduling” chapter of the *Cisco IOS IP SLAs Configuration Guide*.

IP SLA Operation Threshold Monitoring

To support successful service level agreement monitoring, you must have mechanisms that notify you immediately of any possible violation. IP SLAs can send SNMP traps that are triggered by events such as the following:

- Connection loss
- Timeout
- Round-trip time threshold
- Average jitter threshold
- One-way packet loss

- One-way jitter
- One-way mean opinion score (MOS)
- One-way latency

An IP SLA threshold violation can also trigger another IP SLA operation for further analysis. For example, the frequency could be increased or an Internet Control Message Protocol (ICMP) path echo or ICMP path jitter operation could be initiated for troubleshooting.

ICMP Echo

The ICMP echo operation measures the end-to-end response time between a Cisco device and any other device that uses IP. The response time is computed by measuring the time it takes to send an ICMP echo request message to a destination and receive an ICMP echo reply. Many customers use IP SLA ICMP-based operations, in-house ping testing, or ping-based dedicated probes to measure this response time. The IP SLA ICMP echo operation conforms to the same specifications as ICMP ping testing, and both methods result in the same response times.

Related Topics

Analyzing IP Service Levels by Using the ICMP Echo Operation, on page 477

UDP Jitter

Jitter is a simple term that describes interpacket delay variance. When multiple packets are sent consecutively at an interval of 10 ms from source to destination, the destination should receive them 10 ms apart (if the network is behaving correctly). However, if there are delays in the network (such as queuing, arriving through alternate routes, and so on), the time interval between packet arrivals might be more or less than 10 ms. A positive jitter value indicates that the packets arrived more than 10 ms apart. A negative jitter value indicates that the packets arrived less than 10 ms apart. If the packets arrive 12 ms apart, the positive jitter is 2 ms; if the packets arrive 8 ms apart, the negative jitter is 2 ms. For delay-sensitive networks, positive jitter values are undesirable, and a jitter value of 0 is ideal.

In addition to monitoring jitter, the IP SLA UDP jitter operation can be used as a multipurpose data gathering operation. The packets generated by IP SLAs carry sequence information and time stamps from the source and operational target that include packet sending and receiving data. Based on this data, UDP jitter operations measure the following:

- Per-direction jitter (source to destination and destination to source)
- Per-direction packet-loss
- Per-direction delay (one-way delay)
- Round-trip delay (average round-trip time)

Because the paths for the sending and receiving of data can be different (asymmetric), you can use the per-direction data to more readily identify where congestion or other problems are occurring in the network.

The UDP jitter operation generates synthetic (simulated) UDP traffic and sends a number of UDP packets, each of a specified size, sent a specified number of milliseconds apart, from a source router to a target router, at a given frequency. By default, ten packet-frames, each with a payload size of 10 bytes are generated every 10 ms, and the operation is repeated every 60 seconds. You can configure each of these parameters to best simulate the IP service you want to provide.

To provide accurate one-way delay (latency) measurements, time synchronization (as provided by NTP) is required between the source and the target device. Time synchronization is not required for the one-way jitter and packet loss measurements. If the time is not synchronized between the source and target devices, one-way jitter and packet loss data is returned, but values of 0 are returned for the one-way delay measurements provided by the UDP jitter operation.

Related Topics

Analyzing IP Service Levels by Using the UDP Jitter Operation, on page 473

How to Configure IP SLAs Operations

This section does not include configuration information for all available operations as the configuration information details are included in the *Cisco IOS IP SLAs Configuration Guide*. It does include several operations as examples, including configuring the responder, configuring a UDP jitter operation, which requires a responder, and configuring an ICMP echo operation, which does not require a responder. For details about configuring other operations, see the *Cisco IOS IP SLAs Configuration Guide*.

Default Configuration

No IP SLAs operations are configured.

Configuration Guidelines

For information on the IP SLA commands, see the *Cisco IOS IP SLAs Command Reference, Release 12.4T* command reference.

For detailed descriptions and configuration procedures, see the *Cisco IOS IP SLAs Configuration Guide, Release 12.4TL*.

Not all of the IP SLA commands or operations described in the referenced guide are supported on the switch. The switch supports IP service level analysis by using UDP jitter, UDP echo, HTTP, TCP connect, ICMP echo, ICMP path echo, ICMP path jitter, FTP, DNS, and DHCP, as well as multiple operation scheduling and proactive threshold monitoring. It does not support VoIP service levels using the gatekeeper registration delay operations measurements.

Before configuring any IP SLAs application, you can use the **show ip sla application** privileged EXEC command to verify that the operation type is supported on your software image. This is an example of the output from the command:

```
Switch# show ip sla application

        IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
        icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
        dns, udpJitter, dhcp, ftp, udpApp, wspApp

Supported Features:
        IPSLAs Event Publisher

IP SLAs low memory water mark: 33299323
Estimated system max number of entries: 24389
```

```
Estimated number of configurable operations: 24389
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0
Time of last change in whole IP SLAs: *13:04:37.668 UTC Wed Dec 19 2012
```

Configuring the IP SLA Responder

The IP SLA responder is available only on Cisco IOS software-based devices, including some Layer 2 switches that do not support full IP SLA functionality.

Follow these steps to configure the IP SLA responder on the target device (the operational target):

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip sla responder** {**tcp-connect** | **udp-echo**} **ipaddress** *ip-address* **port** *port-number* **Example:** `Switch(config)# ip sla responder udp-echo 172.29.139.134 5000`	Configures the switch as an IP SLA responder. The keywords have these meanings: • **tcp-connect**—Enables the responder for TCP connect operations. • **udp-echo**—Enables the responder for User Datagram Protocol (UDP) echo or jitter operations. • **ipaddress** *ip-address*—Enter the destination IP address. • **port** *port-number*—Enter the destination port number. **Note** The IP address and port number must match those configured on the source device for the IP SLA operation.

	Command or Action	Purpose
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Implementing IP SLA Network Performance Measurement

Follow these steps to implement IP SLA network performance measurement on your switch:

Before you begin

Use the **show ip sla application** privileged EXEC command to verify that the desired operation type is supported on your software image.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip sla** *operation-number* **Example:**	Creates an IP SLA operation, and enters IP SLA configuration mode.

	Command or Action	Purpose
	`Switch(config)# ip sla 10`	
Step 4	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*] **Example:** `Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000`	Configures the IP SLA operation as the operation type of your choice (a UDP jitter operation is used in the example), and enters its configuration mode (UDP jitter configuration mode is used in the example). • *destination-ip-address* | *destination-hostname*—Specifies the destination IP address or hostname. • *destination-port*—Specifies the destination port number in the range from 1 to 65535. • (Optional) **source-ip** {*ip-address* | *hostname*}—Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLA chooses the IP address nearest to the destination • (Optional) **source-port** *port-number*—Specifies the source port number in the range from 1 to 65535. When a port number is not specified, IP SLA chooses an available port. • (Optional) **control**—Enables or disables sending of IP SLA control messages to the IP SLA responder. By default, IP SLA control messages are sent to the destination device to establish a connection with the IP SLA responder • (Optional) **num-packets** *number-of-packets*—Enters the number of packets to be generated. The range is 1 to 6000; the default is 10. • (Optional) **interval** *inter-packet-interval*—Enters the interval between sending packets in milliseconds. The range is 1 to 6000; the default value is 20 ms.
Step 5	**frequency** *seconds* **Example:**	(Optional) Configures options for the SLA operation. This example sets the rate at which a specified IP SLA operation repeats. The

	Command or Action	Purpose
	`Switch(config-ip-sla-jitter)# frequency 45`	range is from 1 to 604800 seconds; the default is 60 seconds.
Step 6	**threshold** *milliseconds* **Example:** `Switch(config-ip-sla-jitter)# threshold 200`	(Optional) Configures threshold conditions. This example sets the threshold of the specified IP SLA operation to 200. The range is from 0 to 60000 milliseconds.
Step 7	**exit** **Example:** `Switch(config-ip-sla-jitter)# exit`	Exits the SLA operation configuration mode (UDP jitter configuration mode in this example), and returns to global configuration mode.
Step 8	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**] **Example:** `Switch(config)# ip sla schedule 10 start-time now life forever`	Configures the scheduling parameters for an individual IP SLA operation. • *operation-number*—Enter the RTR entry number. • (Optional) **life**—Sets the operation to run indefinitely (**forever**) or for a specific number of *seconds*. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour). • (Optional) **start-time**—Enters the time for the operation to begin collecting information: To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month. If no month is entered, the default is the current month. Enter **pending** to select no information collection until a start time is selected. Enter **now** to start the operation immediately. Enter **after** *hh:mm:ss* to show that the operation should start after the entered time has elapsed. • (Optional) **ageout** *seconds*—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to

	Command or Action	Purpose
		2073600 seconds, the default is 0 seconds (never ages out). • (Optional) **recurring**—Set the operation to automatically run every day.
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 10	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 11	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

UDP Jitter Configuration

This example shows how to configure a UDP jitter IP SLA operation:

```
Switch(config)# ip sla 10
Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.

Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
```

```
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

Related Topics

Network Performance Measurement with Cisco IOS IP SLAs, on page 463
Restrictions on SLAs, on page 461

Analyzing IP Service Levels by Using the UDP Jitter Operation

Follow these steps to configure a UDP jitter operation on the source device:

Before you begin

You must enable the IP SLA responder on the target device (the operational target) to configure a UDP jitter operation on the source device.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `Switch(config)# ip sla 10`	Creates an IP SLA operation, and enters IP SLA configuration mode.
Step 4	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable**	Configures the IP SLA operation as a UDP jitter operation, and enters UDP jitter configuration mode.

	Command or Action	Purpose
	| **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*] **Example:** `Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000`	• *destination-ip-address* | *destination-hostname*—Specifies the destination IP address or hostname. • *destination-port*—Specifies the destination port number in the range from 1 to 65535. • (Optional) **source-ip** {*ip-address* | *hostname*}—Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLA chooses the IP address nearest to the destination. • (Optional) **source-port** *port-number*—Specifies the source port number in the range from 1 to 65535. When a port number is not specified, IP SLA chooses an available port. • (Optional) **control**—Enables or disables sending of IP SLA control messages to the IP SLA responder. By default, IP SLA control messages are sent to the destination device to establish a connection with the IP SLA responder. • (Optional) **num-packets** *number-of-packets*—Enters the number of packets to be generated. The range is 1 to 6000; the default is 10. • (Optional) **interval** *inter-packet-interval*—Enters the interval between sending packets in milliseconds. The range is 1 to 6000; the default value is 20 ms.
Step 5	**frequency** *seconds* **Example:** `Switch(config-ip-sla-jitter)# frequency 45`	(Optional) Sets the rate at which a specified IP SLA operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds.
Step 6	**exit** **Example:** `Switch(config-ip-sla-jitter)# exit`	Exits UDP jitter configuration mode, and returns to global configuration mode.

	Command or Action	Purpose
Step 7	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**] **Example:** `Switch(config)# ip sla schedule 10 start-time now life forever`	Configures the scheduling parameters for an individual IP SLA operation. • *operation-number*—Enter the RTR entry number. • (Optional) **life**—Sets the operation to run indefinitely (**forever**) or for a specific number of *seconds*. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour). • (Optional) **start-time**—Enters the time for the operation to begin collecting information: To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month. If no month is entered, the default is the current month. Enter **pending** to select no information collection until a start time is selected. Enter **now** to start the operation immediately. Enter **after** *hh:mm:ss* to show that the operation should start after the entered time has elapsed. • (Optional) **ageout** *seconds*—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds, the default is 0 seconds (never ages out). • (Optional) **recurring**—Set the operation to automatically run every day.
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 9	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.

	Command or Action	Purpose
Step 10	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring a UDP Jitter IP SLA Operation

This example shows how to configure a UDP jitter IP SLA operation:

```
Switch(config)# ip sla 10
Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.

Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

Related Topics

UDP Jitter, on page 466

Analyzing IP Service Levels by Using the ICMP Echo Operation

Follow these steps to configure an ICMP echo operation on the source device:

Before you begin

This operation does not require the IP SLA responder to be enabled.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `Switch(config)# ip sla 10`	Creates an IP SLA operation and enters IP SLA configuration mode.
Step 4	**icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-id*] **Example:** `Switch(config-ip-sla)# icmp-echo 172.29.139.134`	Configures the IP SLA operation as an ICMP Echo operation and enters ICMP echo configuration mode. • *destination-ip-address* | *destination-hostname*—Specifies the destination IP address or hostname. • (Optional) **source-ip** {*ip-address* | *hostname*}—Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLA chooses the IP address nearest to the destination. • (Optional) **source-interface** *interface-id*—Specifies the source interface for the operation.

	Command or Action	Purpose
Step 5	**frequency** *seconds* **Example:** `Switch(config-ip-sla-echo)# frequency 30`	(Optional) Sets the rate at which a specified IP SLA operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds.
Step 6	**exit** **Example:** `Switch(config-ip-sla-echo)# exit`	Exits UDP echo configuration mode, and returns to global configuration mode.
Step 7	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**] **Example:** `Switch(config)# ip sla schedule 5 start-time now life forever`	Configures the scheduling parameters for an individual IP SLA operation. • *operation-number*—Enter the RTR entry number. • (Optional) **life**—Sets the operation to run indefinitely (**forever**) or for a specific number of *seconds*. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour) • (Optional) **start-time**—Enter the time for the operation to begin collecting information: To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month. If no month is entered, the default is the current month. Enter **pending** to select no information collection until a start time is selected. Enter **now** to start the operation immediately. Enter **after** *hh:mm:ss* to indicate that the operation should start after the entered time has elapsed. • (Optional) **ageout** *seconds*—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds; the default is 0 seconds (never ages out). • (Optional) **recurring**—Sets the operation to automatically run every day.

	Command or Action	Purpose
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 9	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 10	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring an ICMP Echo IP SLA Operation

This example shows how to configure an ICMP echo IP SLA operation:

```
Switch(config)# ip sla 12
Switch(config-ip-sla)# icmp-echo 172.29.139.134
Switch(config-ip-sla-echo)# frequency 30
Switch(config-ip-sla-echo)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 22
IP SLAs, Infrastructure Engine-II.

Entry number: 12
Owner:
Tag:
Type of operation to perform: echo
Target address: 2.2.2.2
Source address: 0.0.0.0
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Schedule:
    Operation frequency (seconds): 60
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
```

```
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
History Statistics:
    Number of history Lives kept: 0
    Number of history Buckets kept: 15
    History Filter Type: None
Enhanced History:
```

Related Topics

IP SLA Operation Threshold Monitoring, on page 465

Monitoring IP SLA Operations

The following table describes the commands used to display IP SLA operation configurations and results:

Table 30: Monitoring IP SLA Operations

show ip sla application	Displays global information about Cisco IOS IP SLAs.
show ip sla authentication	Displays IP SLA authentication information.
show ip sla configuration [*entry-number*]	Displays configuration values including all defaults for all IP SLA operations or a specific operation.
show ip sla enhanced-history {**collection-statistics** | **distribution statistics**} [*entry-number*]	Displays enhanced history statistics for collected history buckets or distribution statistics for all IP SLA operations or a specific operation.
show ip sla ethernet-monitor configuration [*entry-number*]	Displays IP SLA automatic Ethernet configuration.
show ip sla group schedule [*schedule-entry-number*]	Displays IP SLA group scheduling configuration and details.
show ip sla history [*entry-number* | **full** | **tabular**]	Displays history collected for all IP SLA operations.
show ip sla mpls-lsp-monitor {**collection-statistics** | **configuration** | **ldp operational-state** | **scan-queue** | **summary** [*entry-number*] | **neighbors**}	Displays MPLS label switched path (LSP) Health Monitor operations.
show ip sla reaction-configuration [*entry-number*]	Displays the configured proactive threshold monitoring settings for all IP SLA operations or a specific operation.
show ip sla reaction-trigger [*entry-number*]	Displays the reaction trigger information for all IP SLA operations or a specific operation.
show ip sla responder	Displays information about the IP SLA responder.
show ip sla statistics [*entry-number* | **aggregated** | **details**]	Displays current or aggregated operational status and statistics.

Monitoring IP SLA Operation Examples

The following example shows all IP SLAs by application:

```
Switch# show ip sla application

        IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
        icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
        dns, udpJitter, dhcp, ftp, udpApp, wspApp

Supported Features:
        IPSLAs Event Publisher

IP SLAs low memory water mark: 33299323
Estimated system max number of entries: 24389

Estimated number of configurable operations: 24389
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0
Time of last change in whole IP SLAs: *13:04:37.668 UTC Wed Dec 19 2012
```

The following example shows all IP SLA distribution statistics:

```
Switch# show ip sla enhanced-history distribution-statistics

Point by point Enhanced History
Entry    = Entry Number
Int      = Aggregation Interval
BucI     = Bucket Index
StartT   = Aggregation Start Time
Pth      = Path index
Hop      = Hop in path index
Comps    = Operations completed
OvrTh    = Operations completed over thresholds
SumCmp   = Sum of RTT (milliseconds)
SumCmp2L = Sum of RTT squared low 32 bits (milliseconds)
SumCmp2H = Sum of RTT squared high 32 bits (milliseconds)
TMax     = RTT maximum (milliseconds)
TMin     = RTT minimum (milliseconds)

Entry Int BucI StartT     Pth Hop Comps OvrTh SumCmp     SumCmp2L   SumCmp2H   T
Max    TMin
```

Additional References

Related Documents

Related Topic	Document Title
Cisco Medianet Metadata Guide	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mdata/configuration/15-sy/mdata-15sy-book/metadata-framework.pdf

Related Topic	Document Title
Cisco Media Services Proxy Configuration Guide	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/msp/configuration/15-mt/msp-15-mt-book.pdf
Cisco Mediatrace and Cisco Performance Monitor Configuration Guide	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/media_monitoring/configuration/15-mt/mm-15-mt-book/mm-mediatrace.html

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
None	-

MIBs

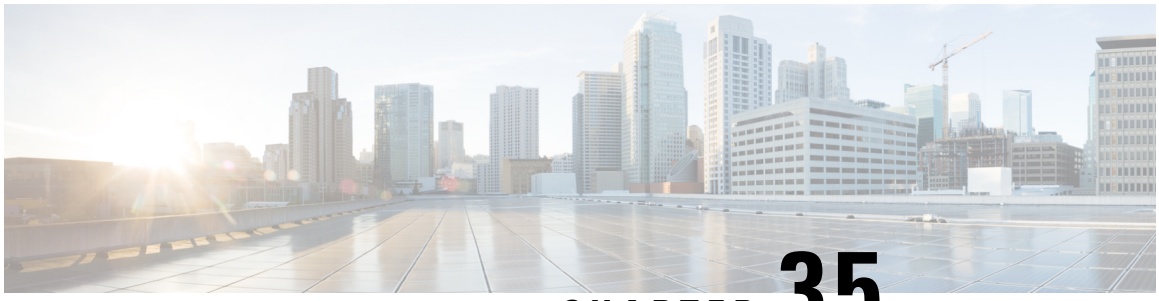
MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for Service Level Agreements

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 35

Configuring Local Policies

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring Local Policies

- The policy map attributes supported on the switch are QoS, VLAN, session timeout, and ACL.
- Apple iphone 6s will get classified as "workstation" after HTTP profiling.

Related Topics

Creating a Parameter Map (CLI), on page 489
Creating a Class Map (CLI), on page 491
Creating a Policy Map (CLI), on page 491
Applying a Local Policy for a Device on a WLAN (CLI), on page 492
Creating an Interface Template (CLI), on page 489
Information About Configuring Local Policies, on page 486
Creating a Service Template (GUI), on page 494

Creating a Policy Map (GUI), on page 495
Applying Local Policies to WLAN (GUI), on page 496

Information About Configuring Local Policies

Local policies can profile devices based on HTTP and DHCP to identify the end devices on the network. Users can configure device-based policies and enforce the policies per user or per device policy on the network.

Local policies allow profiling of mobile devices and basic onboarding of the profiled devices to a specific VLAN. They also assign ACL and QoS or configure session timeouts. You can configure local policies as two separate components:

- Defining policy attributes as service templates specific to clients joining the network and applying policy match criteria.
- Applying match criteria to the policy.

The following policy match attributes are used for configuring local policies:

- Device—Defines the type of device. Windows-based computer, Smart phone, Apple devices such as iPad and iPhone.
- Username—Defines the username of the user.
- User role—Defines the user type or the user group the user belongs to, such as a student or employee.
- MAC—Defines the mac-address of the end point.
- MAC OUI—Defines the mac-address OUI.

Once the switch has a match corresponding to these parameters per end point, the policy can be added. Policy enforcement allows basic device on-boarding of mobile devices based on the following session attributes:

- VLAN
- QoS
- ACL
- Session timeout

You can configure these policies and enforce end points with specified policies. The wireless clients are profiled based on MAC OUI, DHCP, and HTTP user agent (valid Internet is required for successful HTTP profiling)MAC OUI and DHCP. The switch uses these attributes and predefined classification profiles to identify devices.

Replacing Default Profile Text File

If a new device is not classified, contact the Cisco support team with the device MAC address. The Cisco support team will provide a new **dc_default_profile.txt** file with the MAC address included in the file. You need to replace the **dc_default_profile.txt** file with the earlier file. Follow these steps to change the **dc_default_profile.txt** file:

1. Stop device classifier by entering this command:

   switch**(config)# no device classifier**

2. Copy the file by entering this command:

   switch# **device classifier profile location** *filepath*

3. Start the device classifier by entering this command:

   switch**(config)# device classifier**

Disabling session monitor on trunk ports

On uplink trunk ports, you should not create any session monitoring. By default, session monitoring is enabled. You should disable session monitoring.

1. Enter into global configuration mode by entering this command:

   switch# **configure terminal**

2. Enter into interface configuration mode by entering this command:

   switch**(config)# interface** *interface-id*

3. Disable session monitoring by entering this command:

   switch**(config-if)# no access-session monitor**

Related Topics

Creating a Parameter Map (CLI), on page 489
Creating a Class Map (CLI), on page 491
Creating a Policy Map (CLI), on page 491
Applying a Local Policy for a Device on a WLAN (CLI), on page 492
Creating an Interface Template (CLI), on page 489
Restrictions for Configuring Local Policies, on page 485
Monitoring Local Policies, on page 496
Examples: Local Policies Configuration, on page 497
Creating a Service Template (GUI), on page 494
Creating a Policy Map (GUI), on page 495
Applying Local Policies to WLAN (GUI), on page 496

How to Configure Local Policies

Configuring Local Policies (CLI)

To configure local policies, complete these procedures:

1. Create a service template.
2. Create an interface template.
3. Create a parameter map.
4. Create a policy map.
5. Apply a local policy on a WLAN.

Creating a Service Template (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 2	**service-template** *service-template-name*
	Example:
	`Switch(config)# service-template cisco-phone-template`
	`Switch(config-service-template)#`
		Enters service template configuration mode.

Step 3	**access-group** *acl_list* **Example:** `Switch(config-service-template)# access-group foo-acl`	Specifies the access list to be applied.
Step 4	**vlan** *vlan_id* **Example:** `Switch(config-service-template)# vlan 100`	Specifies VLAN ID. You can specify a value from 1 to 4094.
Step 5	**absolute-timer** *seconds* **Example:** `Switch(config-service-template)# absolute-timer 20`	Specifies session timeout value for service template. You can specify a value from 1 to 65535.
Step 6	**service-policy qos** {**input** | **output**} **Example:** `Switch(config-service-template)# service-policy qos input foo-qos`	Configures QoS policies for the client.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating an Interface Template (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 2	**template** *interface-template-name*
	Example:
	`Switch(config)# template cisco-phone-template`
	`Switch(config-template)#`
		Enters interface template configuration mode.

Step 3	**switchport mode access** **Example:** `Switch(config-template)# switchport mode access`	Sets the interface as a nontrunking nontagged single-VLAN Ethernet interface. An access port can carry traffic in one VLAN only. By default, an access port carries traffic for VLAN1.
Step 4	**switchport voice vlan** *vlan_id* **Example:** `Switch(config-template)# switchport voice vlan 20`	Specifies to forward all voice traffic through the specified VLAN. You can specify a value from 1 to 4094.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Information About Configuring Local Policies, on page 486
Restrictions for Configuring Local Policies, on page 485
Monitoring Local Policies, on page 496
Examples: Local Policies Configuration, on page 497

Creating a Parameter Map (CLI)

Parameter map is preferred to use than class map.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Switch# configure terminal`	
Step 2	**parameter-map type subscriber attribute-to-service** *parameter-map-name* **Example:** `Switch(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para`	Specifies the parameter map type and name.
Step 3	*map-index* **map** { **device-type** | **mac-address** | **oui** | **user-role** | **username**} {**eq** | **not-eq** | **regex** *filter-name* } **Example:** `Switch(config-parameter-map-filter)# 10 map device-type eq "WindowsXP-Workstation"`	Specifies parameter map attribute filter criteria.

Step 4	**service-template** *service-template-name*
	Example:
	`Switch(config-parameter-map-filter-submode)# service-template cisco-phone-template`
	`Switch(config-parameter-map-filter-submode)#`
		Enters service template configuration mode.

Step 5	**interface-template** *interface-template-name*
	Example:
	`Switch(config-parameter-map-filter-submode)# interface-template cisco-phone-template`
	`Switch(config-parameter-map-filter-submode)#`
		Enters service template configuration mode.

Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Information About Configuring Local Policies, on page 486
Restrictions for Configuring Local Policies, on page 485
Monitoring Local Policies, on page 496
Examples: Local Policies Configuration, on page 497

Creating a Class Map (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**class-map type control subscriber** *class-map-name* { **match-all** | **match-any** | **match-first** } **Example:** `Switch(config)# class-map type control subscriber CLASS_AC_1 match-all`	Specifies the class map type and name.
Step 3	**match** {**device-type** | **mac-address** | **oui** | **username** | **userrole**} *filter-type-name* **Example:** `Switch(config-class-map)# match device-type Cisco-IP-Phone-7961`	Specifies class map attribute filter criteria.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Information About Configuring Local Policies, on page 486
Restrictions for Configuring Local Policies, on page 485
Monitoring Local Policies, on page 496
Examples: Local Policies Configuration, on page 497

Creating a Policy Map (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**policy-map type control subscriber** *policy-map-name* **Example:**	Specifies the policy map type.

	Command or Action	Purpose
	`Switch(config)# policy-map type control subscriber Aironet-Policy`	
Step 3	**event identity-update** {**match-all** | **match-first**} **Example:** `Switch(config-policy-map)# event identity-update match-all`	Specifies match criteria to the policy map.
Step 4	*class_number* **class** {*class_map_name* | **always** } {**do-all** | **do-until-failure** | **do-until-success**} **Example:** `Switch(config-class-control-policymap)# 1 class local_policy1_class do-until-success`	Configures the local profiling policy class map number and specifies how to perform the action. The class map configuration mode includes the following command options: • **always**—Executes without doing any matching but return success. • **do-all**—Executes all the actions. • **do-until-failure**—Execute all the actions until any match failure is encountered. This is the default value. • **do-until-success**—Execute all the actions until any match success happens.
Step 5	*action-index* **map attribute-to-service table** *parameter-map-name* **Example:** `Switch(config-policy-map)# 10 map attribute-to-service table Aironet-Policy-para`	Specifies parameter map table to be used.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Information About Configuring Local Policies, on page 486
Restrictions for Configuring Local Policies, on page 485
Monitoring Local Policies, on page 496
Examples: Local Policies Configuration, on page 497

Applying a Local Policy for a Device on a WLAN (CLI)

Before you begin

If the service policy contains any device type-based rules in the parameter map, ensure that the device classifier is already enabled.

Note You should use the **device classification** command to classify the device for it to be displayed correctly on the show command output.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name* **Example:** `Switch(config)# wlan wlan1`	Enters WLAN configuration mode.
Step 3	**service-policy type control subscriber** *policymapname* **Example:** `Switch(config-wlan)# service-policy type control subscriber Aironet-Policy`	Applies local policy to WLAN.
Step 4	**profiling local http (optional)** **Example:** `Switch(config-wlan)# profiling local http`	Enables only profiling of devices based on HTTP protocol (optional).
Step 5	**profiling radius http (optional)** **Example:** `Switch(config-wlan)# profiling radius http`	Enables profiling of devices on ISE (optional).
Step 6	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Specifies not to shut down the WLAN.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Information About Configuring Local Policies, on page 486
Restrictions for Configuring Local Policies, on page 485
Monitoring Local Policies, on page 496
Examples: Local Policies Configuration, on page 497

Configuring Local Policies (GUI)

To configure local policies, complete these procedures:

Procedure

	Command or Action	Purpose
Step 1	Create a service template.	
Step 2	Create a policy map.	
Step 3	Apply a local policy that you have created to a WLAN.	

Creating a Service Template (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Local Policies** > **Service Template** to open the **Service Template** page.

Step 2 Create a new template as follows:

a) Click **New** to open the **Service Template > New** page.
b) In the Service Template name text box, enter the new service template name.
c) In the VLAN ID text box, enter the VLAN identifier that has to be associated with the policy. The value ranges from 1 to 4094.
d) In the Session timeout text box, enter the maximum amount of time, in seconds, after which a client is forced to reauthenticate. The value ranges from 1 to 65535 seconds.
e) From the Access control list drop-down list, choose the access control list to be mapped to the policy.
f) From the Ingress QoS drop-down list, choose the ingress QoS policy to be applied.
g) From the Egress QoS drop-down list, choose the egress QoS policy to be applied.
h) Click **Apply** to save the configuration.

Step 3 Edit a service template as follows:

a) From the **Service Template** page, click the service template to open the **Service Template > Edit** page.
b) In the VLAN ID text box, enter the VLAN identifier that has to be associated with the policy. The value ranges from 1 to 4094.
c) In the Session timeout text box, enter the maximum amount of time, in seconds, after which a client is forced to reauthenticate. The value ranges from 1 to 65535 seconds.
d) From the Access control list drop-down list, choose the access control list to be mapped to the policy.
e) From the Ingress QoS drop-down list, choose the ingress QoS policy to be applied.
f) From the Egress QoS drop-down list, choose the egress QoS policy to be applied.
g) Click **Apply** to save the configuration.

Step 4 Remove a service template as follows:

a) From the **Service Template** page, select the service template.
b) Click **Remove**.
c) Click **Apply** to save the configuration.

Related Topics

Information About Configuring Local Policies, on page 486
Restrictions for Configuring Local Policies, on page 485
Monitoring Local Policies, on page 496
Examples: Local Policies Configuration, on page 497

Creating a Policy Map (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Local Policies** > **Policy Map** to open the **Policy Map** page.

Step 2 Create a new policy map as follows:

a) Click **New** to open the **Policy Map > New** page.
b) In the Policy Map name text box, enter the new policy map name.
c) Click **Add** to open the Match Criteria area.
d) From the Device Type drop-down list, choose the device type. The match criteria for the device type can be eq, not-eq, or regex with respect to the device type you are choosing.
e) From the User Role drop-down list, select the match criteria as eq, not-eq, or regex and enter the user type or user group of the user, for example, student, teacher, and so on.
f) From the Service Template drop-down list, choose the service template to be mapped to the policy.
g) Click **Add**. The match criteria is added to the Match Criteria Lists.
h) In the Match Criteria Lists area, click **Add** to add the match criteria to the policy.
i) Click **Apply** to save the configuration.

Step 3 Edit a policy map as follows:

a) In the **Policy Map** page, select the policy map that you want to edit, and click **Edit** to open the **Policy Map > Edit** page.
b) In the Match Criteria area, choose the device type from the Device Type drop-down list. The match criteria for the device type can be eq, not-eq, or regex with respect to the device type you are choosing.
c) In the Match Criteria area, choose the user role from the User Role drop-down list. Select the match criteria as eq, not-eq, or regex and enter the user type or user group of the user
d) From the Service Template drop-down list, choose the service template to be mapped to the policy.
e) Click **Ok** to save the configuration or **Cancel** to discard the configuration.
f) Click **Add** to add more match criteria based on device type, user role, and service template to the policy.
g) In the Match Criteria Lists area, select the match criteria and click **Move to** to move the match criteria with respect to a value entered in the row text box.
h) Select the match criteria and click **Move up** to move the match criteria up in the list.
i) Select the match criteria and click **Move down** to move the match criteria down in the list.
j) Select the match criteria and click **Remove** to remove the match criteria from the policy map list.
k) Click **Apply** to save the configuration.

Step 4 Remove a policy map as follows:

a) From the **Policy Map** page, select the policy map.
b) Click **Remove**.
c) Click **Apply** to save the configuration.

Related Topics

Information About Configuring Local Policies, on page 486
Restrictions for Configuring Local Policies, on page 485
Monitoring Local Policies, on page 496
Examples: Local Policies Configuration, on page 497

Applying Local Policies to WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **WLAN** to open the **WLANs** page.
Step 2 Click the corresponding WLAN profile. The **WLANs > Edit** page is displayed.
Step 3 Click the **Policy-Mapping** tab.
Step 4 Check the **Device Classification** check box to enable classification based on device type.
Step 5 From the Local Subscriber Policy drop-down list, choose the policy that has to be applied for the WLAN.
Step 6 Select **Local HTTP Profiling** to enable profiling on devices based on HTTP (optional).
Step 7 Select **Radius HTTP Profiling** to enable profiling on devices based on RADIUS (optional).
Step 8 Click **Apply** to save the configuration.

Related Topics

Information About Configuring Local Policies, on page 486
Restrictions for Configuring Local Policies, on page 485
Monitoring Local Policies, on page 496
Examples: Local Policies Configuration, on page 497

Monitoring Local Policies

The following commands can be used to monitor local policies configured on the switch.

Table 31: Monitoring Local Policies Command

Command	Purpose
show access-session	Displays the summary of access session with authorization status, method and domain for each client or MAC address displayed.
show access-session cache	Displays the latest classification for the client.
show device classifier attached detail	Displays the latest classification for the client based on parameters such as Mac, DHCP, or HTTP.

show access-session mac *mac-address* **details**	Displays the policy mapped, service template used, and attributes for the client. **Note** If the **show access-session detail** command output is not displaying session timeout details, you should enable client profiling with session timeout in client access session and then run the **show access-session mac** *mac-address* **details** command to see the session timeout details.
show access-session mac *mac-address* **policy**	Displays the policy mapped, service template used, and attributes for the client. In addition, you can view the **Resultant Policy** that displays the following information: • The final attributes applied to the session when the session has locally configured attributes. • Attributes applied from the server.

Related Topics

Creating a Parameter Map (CLI), on page 489
Creating a Class Map (CLI), on page 491
Creating a Policy Map (CLI), on page 491
Applying a Local Policy for a Device on a WLAN (CLI), on page 492
Creating an Interface Template (CLI), on page 489
Information About Configuring Local Policies, on page 486
Creating a Service Template (GUI), on page 494
Creating a Policy Map (GUI), on page 495
Applying Local Policies to WLAN (GUI), on page 496

Examples: Local Policies Configuration

This example shows how to create service template:

```
Switch(config)# service-template test3
Switch(config-service-template)# access-group josephacl
Switch(config-service-template)# vlan 137
Switch(config-service-template)# absolute-timer 500
Switch(config-service-template)#  service-policy qos input qosingress
Switch(config-service-template)# end
```

This example shows how to create parameter map:

```
Switch(config)# parameter-map type subscriber attribute-to-service apple-tsim-param
Switch(config-parameter-map)# 1 map device-type eq "Apple-Device"
Switch(config-parameter-map)# 1 service-template test1
Switch(config-parameter-map)# 2 map device-type eq "Apple-Ipad"
Switch(config-parameter-map)# 1 service-template test2
Switch(config-parameter-map)# 3 map device-type eq "Android"
```

```
Switch(config-parameter-map)# 1 service-template test3
Switch(config-parameter-map)# end
```

Note At the end of each configuration command line, enter CTRL Z to execute the command and proceed to the next line.

This example shows how to create interface template:

```
Switch# configure terminal
Switch(config)#template cisco-phone-template
Switch(config-template)#switchport mode access
Switch(config-template)#switchport voice vlan 20
Switch(config-template)# end
```

This example shows how to create parameter map:

```
Switch# configure terminal
Switch(config)#parameter-map type subscriber attribute-to-service param-wired
Switch(config-parameter-map-filter)#10 map device-type regex Cisco-IP-Phone
Switch(config-parameter-map-filter-submode)#10 interface-template cisco-phone-template
Switch(config-parameter-map)# end
```

This example shows how to create policy map:

```
Switch(config)# policy-map type control subscriber apple-tsim
Switch(config-policy-map)# event identity-update match-all
Switch(config-policy-map)# 1 class always do-until-failure
Switch(config-policy-map)# 1 map attribute-to-service table apple-tsim-param
Switch(config-policy-map)# end
```

This example shows how to apply policy to a device on a WLAN:

```
Switch(config)# wlan wlan1
Switch(config-wlan)# client vlan VLAN0054
Switch(config-wlan)# profiling local http
Switch(config-wlan)# service-policy type control subscriber apple-tsim
Switch(config-wlan)# no shutdown
Switch# end
```

Related Topics

Creating a Parameter Map (CLI), on page 489
Creating a Class Map (CLI), on page 491
Creating a Policy Map (CLI), on page 491
Applying a Local Policy for a Device on a WLAN (CLI), on page 492
Creating an Interface Template (CLI), on page 489
Information About Configuring Local Policies, on page 486
Creating a Service Template (GUI), on page 494
Creating a Policy Map (GUI), on page 495
Applying Local Policies to WLAN (GUI), on page 496

Additional References for Configuring Local Policies

Related Documents

Related Topic	Document Title
Security commands	*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

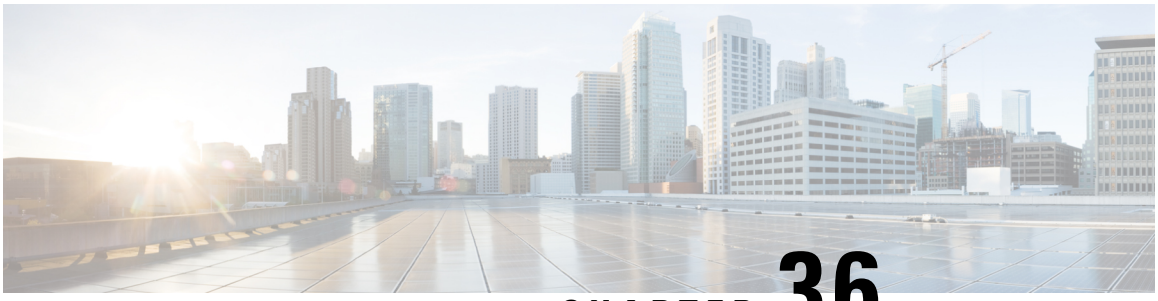
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History for Performing Local Policies Configuration

Release	Feature Information
Cisco IOS XE 3E	This feature was introduced.



CHAPTER 36

Configuring SPAN and RSPAN

Prerequisites for SPAN and RSPAN

SPAN

- You can limit SPAN traffic to specific VLANs by using the **filter vlan** keyword. If a trunk port is being monitored, only traffic on the VLANs specified with this keyword is monitored. By default, all VLANs are monitored on a trunk port.

RSPAN

- We recommend that you configure an RSPAN VLAN before you configure an RSPAN source or a destination session.

Restrictions for SPAN and RSPAN

SPAN

The restrictions for SPAN are as follows:

- On each switch, you can configure 66 sessions. A maximum of source sessions can be configured and the remaining sessions can be configured as RSPAN destinations sessions. A source session is either a local SPAN session or an RSPAN source session.
- For SPAN sources, you can monitor traffic for a single port or VLAN or a series or range of ports or VLANs for each session. You cannot mix source ports and source VLANs within a single SPAN session.

- The destination port cannot be a source port; a source port cannot be a destination port.
- You cannot have two SPAN sessions using the same destination port.
- When you configure a switch port as a SPAN destination port, it is no longer a normal switch port; only monitored traffic passes through the SPAN destination port.
- Entering SPAN configuration commands does not remove previously configured SPAN parameters. You must enter the **no monitor session** {*session_number* | **all** | **local** | **remote**} global configuration command to delete configured SPAN parameters.
- For local SPAN, outgoing packets through the SPAN destination port carry the original encapsulation headers—untagged, ISL, or IEEE 802.1Q—if the **encapsulation replicate** keywords are specified. If the keywords are not specified, the packets are sent in native form.
- You can configure a disabled port to be a source or destination port, but the SPAN function does not start until the destination port and at least one source port or source VLAN are enabled.
- You cannot mix source VLANs and filter VLANs within a single SPAN session.

Traffic monitoring in a SPAN session has the following restrictions:

- Sources can be ports or VLANs, but you cannot mix source ports and source VLANs in the same session.
- Wireshark does not capture egress packets when egress span is active.
- You can run both a local SPAN and an RSPAN source session in the same switch or switch stack. The switch or switch stack supports a total of 66 source and RSPAN destination sessions.
- You can configure two separate SPAN or RSPAN source sessions with separate or overlapping sets of SPAN source ports and VLANs. Both switched and routed ports can be configured as SPAN sources and destinations.
- You can have multiple destination ports in a SPAN session, but no more than 64 destination ports per switch stack.
- SPAN sessions do not interfere with the normal operation of the switch. However, an oversubscribed SPAN destination, for example, a 10-Mb/s port monitoring a 100-Mb/s port, can result in dropped or lost packets.
- When SPAN or RSPAN is enabled, each packet being monitored is sent twice, once as normal traffic and once as a monitored packet. Monitoring a large number of ports or VLANs could potentially generate large amounts of network traffic.
- You can configure SPAN sessions on disabled ports; however, a SPAN session does not become active unless you enable the destination port and at least one source port or VLAN for that session.
- The switch does not support a combination of local SPAN and RSPAN in a single session.
    - An RSPAN source session cannot have a local destination port.
    - An RSPAN destination session cannot have a local source port.
    - An RSPAN destination session and an RSPAN source session that are using the same RSPAN VLAN cannot run on the same switch or switch stack.

RSPAN

The restrictions for RSPAN are as follows:

- RSPAN does not support BPDU packet monitoring or other Layer 2 switch protocols.
- The RSPAN VLAN is configured only on trunk ports and not on access ports. To avoid unwanted traffic in RSPAN VLANs, make sure that the VLAN remote-span feature is supported in all the participating switches.
- RSPAN VLANs are included as sources for port-based RSPAN sessions when source trunk ports have active RSPAN VLANs. RSPAN VLANs can also be sources in SPAN sessions. However, since the switch does not monitor spanned traffic, it does not support egress spanning of packets on any RSPAN VLAN identified as the destination of an RSPAN source session on the switch.
-
- If you enable VTP and VTP pruning, RSPAN traffic is pruned in the trunks to prevent the unwanted flooding of RSPAN traffic across the network for VLAN IDs that are lower than 1005.
- To use RSPAN, the switch must be running the LAN Base image.

Information About SPAN and RSPAN

SPAN and RSPAN

You can analyze network traffic passing through ports or VLANs by using SPAN or RSPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports or source VLANs to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports or VLANs. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN or RSPAN session, destination ports do not receive or forward traffic.

Only traffic that enters or leaves source ports or traffic that enters or leaves source VLANs can be monitored by using SPAN; traffic routed to a source VLAN cannot be monitored. For example, if incoming traffic is being monitored, traffic that gets routed from another VLAN to the source VLAN cannot be monitored; however, traffic that is received on the source VLAN and routed to another VLAN can be monitored.

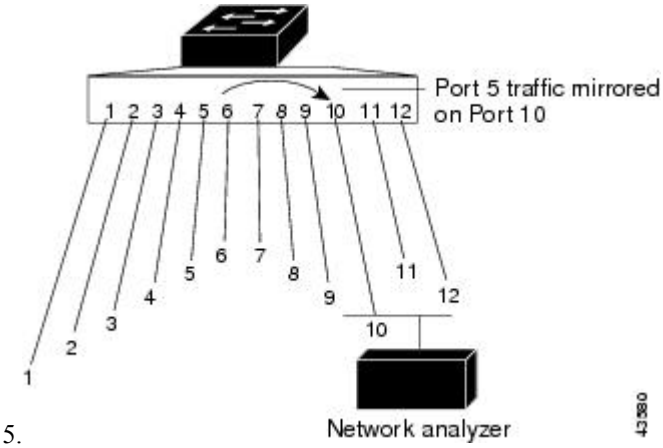
You can use the SPAN or RSPAN destination port to inject traffic from a network security device. For example, if you connect a Cisco Intrusion Detection System (IDS) sensor appliance to a destination port, the IDS device can send TCP reset packets to close down the TCP session of a suspected attacker.

Local SPAN

Local SPAN supports a SPAN session entirely within one switch; all source ports or source VLANs and destination ports are in the same switch or switch stack. Local SPAN copies traffic from one or more source ports in any VLAN or from one or more VLANs to a destination port for analysis.

Figure 35: Example of Local SPAN Configuration on a Single Device

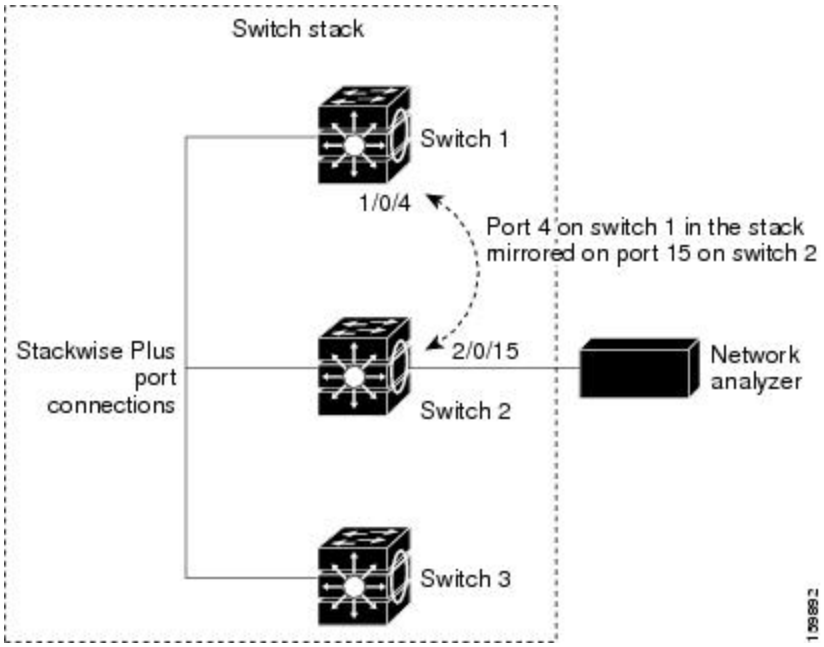
All traffic on port 5 (the source port) is mirrored to port 10 (the destination port). A network analyzer on port 10 receives all network traffic from port 5 without being physically attached to port



5.

Figure 36: Example of Local SPAN Configuration on a Device Stack

This is an example of a local SPAN in a switch stack, where the source and destination ports reside on different stack members.



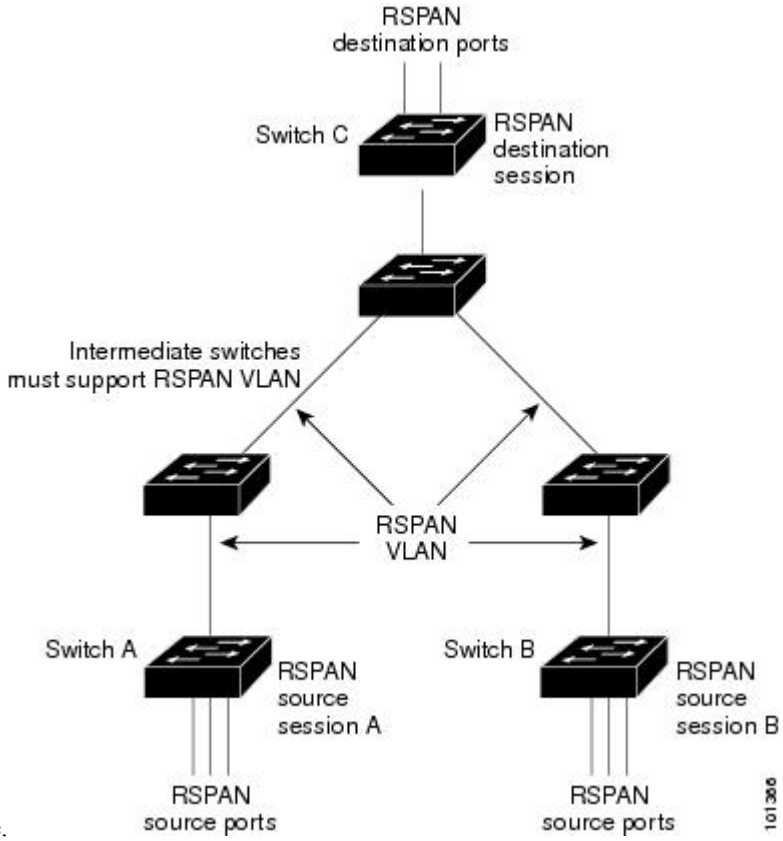
Remote SPAN

RSPAN supports source ports, source VLANs, and destination ports on different switches (or different switch stacks), enabling remote monitoring of multiple switches across your network.

Figure 37: Example of RSPAN Configuration

The figure below shows source ports on Switch A and Switch B. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches.

The RSPAN traffic from the source ports or VLANs is copied into the RSPAN VLAN and forwarded over trunk ports carrying the RSPAN VLAN to a destination session monitoring the RSPAN VLAN. Each RSPAN source switch must have either ports or VLANs as RSPAN sources. The destination is always a physical port, as shown on Switch C in the figure.



SPAN and RSPAN Concepts and Terminology

- SPAN Sessions
- Monitored Traffic
- Source Ports
- Source VLANs
- VLAN Filtering
- Destination Port
- RSPAN VLAN

SPAN Sessions

SPAN sessions (local or remote) allow you to monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports.

A local SPAN session is an association of a destination port with source ports or source VLANs, all on a single network device. Local SPAN does not have separate source and destination sessions. Local SPAN

sessions gather a set of ingress and egress packets specified by the user and form them into a stream of SPAN data, which is directed to the destination port.

RSPAN consists of at least one RSPAN source session, an RSPAN VLAN, and at least one RSPAN destination session. You separately configure RSPAN source sessions and RSPAN destination sessions on different network devices. To configure an RSPAN source session on a device, you associate a set of source ports or source VLANs with an RSPAN VLAN. The output of this session is the stream of SPAN packets that are sent to the RSPAN VLAN. To configure an RSPAN destination session on another device, you associate the destination port with the RSPAN VLAN. The destination session collects all RSPAN VLAN traffic and sends it out the RSPAN destination port.

An RSPAN source session is very similar to a local SPAN session, except for where the packet stream is directed. In an RSPAN source session, SPAN packets are relabeled with the RSPAN VLAN ID and directed over normal trunk ports to the destination switch.

An RSPAN destination session takes all packets received on the RSPAN VLAN, strips off the VLAN tagging, and presents them on the destination port. The session presents a copy of all RSPAN VLAN packets (except Layer 2 control packets) to the user for analysis.

A single RSPAN session with multiple source and destination ports can be in the same session but more than one source session with the source being the same remote vlan is not allowed.

Traffic monitoring in a SPAN session has these restrictions:

- Sources can be ports or VLANs, but you cannot mix source ports and source VLANs in the same session.
- You can run both a local SPAN and an RSPAN source session in the same switch or switch stack. The switch or switch stack supports a total of 66 source and RSPAN destination sessions.
- You can configure two separate SPAN or RSPAN source sessions with separate or overlapping sets of SPAN source ports and VLANs. Both switched and routed ports can be configured as SPAN sources and destinations.
- You can have multiple destination ports in a SPAN session, but no more than 64 destination ports per switch stack.
- SPAN sessions do not interfere with the normal operation of the switch. However, an oversubscribed SPAN destination, for example, a 10-Mb/s port monitoring a 100-Mb/s port, can result in dropped or lost packets.
- When SPAN or RSPAN is enabled, each packet being monitored is sent twice, once as normal traffic and once as a monitored packet. Therefore monitoring a large number of ports or VLANs could potentially generate large amounts of network traffic.
- You can configure SPAN sessions on disabled ports; however, a SPAN session does not become active unless you enable the destination port and at least one source port or VLAN for that session.
- The switch does not support a combination of local SPAN and RSPAN in a single session.
    - An RSPAN source session cannot have a local destination port.
    - An RSPAN destination session cannot have a local source port.
    - An RSPAN destination session and an RSPAN source session that are using the same RSPAN VLAN cannot run on the same switch or switch stack.

Monitored Traffic

SPAN sessions can monitor these traffic types:

- Receive (Rx) SPAN—Receive (or ingress) SPAN monitors as much as possible all of the packets received by the source interface or VLAN before any modification or processing is performed by the switch. A copy of each packet received by the source is sent to the destination port for that SPAN session.

  Packets that are modified because of routing or Quality of Service (QoS)—for example, modified Differentiated Services Code Point (DSCP)—are copied before modification.

  Features that can cause a packet to be dropped during receive processing have no effect on ingress SPAN; the destination port receives a copy of the packet even if the actual incoming packet is dropped. These features include IP standard and extended input Access Control Lists (ACLs), ingress QoS policing, VLAN ACLs, and egress QoS policing.

- Transmit (Tx) SPAN—Transmit (or egress) SPAN monitors as much as possible all of the packets sent by the source interface after all modification and processing is performed by the switch. A copy of each packet sent by the source is sent to the destination port for that SPAN session. The copy is provided after the packet is modified.

  Packets that are modified because of routing (for example, with modified time-to-live (TTL), MAC address, or QoS values) are duplicated (with the modifications) at the destination port.

  Features that can cause a packet to be dropped during transmit processing also affect the duplicated copy for SPAN. These features include IP standard and extended output ACLs and egress QoS policing.

- Both—In a SPAN session, you can also monitor a port or VLAN for both received and sent packets. This is the default.

The default configuration for local SPAN session ports is to send all packets untagged. However, when you enter the **encapsulation replicate** keywords while configuring a destination port, these changes occur:

- Packets are sent on the destination port with the same encapsulation (untagged or IEEE 802.1Q) that they had on the source port.
- Packets of all types, including BPDU and Layer 2 protocol packets, are monitored.

Therefore, a local SPAN session with encapsulation replicate enabled can have a mixture of untagged and IEEE 802.1Q tagged packets appear on the destination port.

Switch congestion can cause packets to be dropped at ingress source ports, egress source ports, or SPAN destination ports. In general, these characteristics are independent of one another. For example:

- A packet might be forwarded normally but dropped from monitoring due to an oversubscribed SPAN destination port.
- An ingress packet might be dropped from normal forwarding, but still appear on the SPAN destination port.
- An egress packet dropped because of switch congestion is also dropped from egress SPAN.

In some SPAN configurations, multiple copies of the same source packet are sent to the SPAN destination port. For example, a bidirectional (both Rx and Tx) SPAN session is configured for the Rx monitor on port A and Tx monitor on port B. If a packet enters the switch through port A and is switched to port B, both incoming and outgoing packets are sent to the destination port. Both packets are the same unless a Layer 3 rewrite occurs, in which case the packets are different because of the packet modification.

Source Ports

A source port (also called a monitored port) is a switched or routed port that you monitor for network traffic analysis.

In a local SPAN session or RSPAN source session, you can monitor source ports or VLANs for traffic in one or both directions.

The switch supports any number of source ports (up to the maximum number of available ports on the switch) and any number of source VLANs (up to the maximum number of VLANs supported).

However, the switch supports a maximum of two sessions (local or RSPAN) with source ports or VLANs. You cannot mix ports and VLANs in a single session.

A source port has these characteristics:

- It can be monitored in multiple SPAN sessions.
- Each source port can be configured with a direction (ingress, egress, or both) to monitor.
- It can be any port type (for example, EtherChannel, Gigabit Ethernet, and so forth).
- For EtherChannel sources, you can monitor traffic for the entire EtherChannel or individually on a physical port as it participates in the port channel.
- It can be an access port, trunk port, routed port, or voice VLAN port.
- It cannot be a destination port.
- Source ports can be in the same or different VLANs.
- You can monitor multiple source ports in a single session.

Source VLANs

VLAN-based SPAN (VSPAN) is the monitoring of the network traffic in one or more VLANs. The SPAN or RSPAN source interface in VSPAN is a VLAN ID, and traffic is monitored on all the ports for that VLAN.

VSPAN has these characteristics:

- All active ports in the source VLAN are included as source ports and can be monitored in either or both directions.
- On a given port, only traffic on the monitored VLAN is sent to the destination port.
- If a destination port belongs to a source VLAN, it is excluded from the source list and is not monitored.
- If ports are added to or removed from the source VLANs, the traffic on the source VLAN received by those ports is added to or removed from the sources being monitored.
- You cannot use filter VLANs in the same session with VLAN sources.
- You can monitor only Ethernet VLANs.

VLAN Filtering

When you monitor a trunk port as a source port, by default, all VLANs active on the trunk are monitored. You can limit SPAN traffic monitoring on trunk source ports to specific VLANs by using VLAN filtering.

- VLAN filtering applies only to trunk ports or to voice VLAN ports.

- VLAN filtering applies only to port-based sessions and is not allowed in sessions with VLAN sources.
- When a VLAN filter list is specified, only those VLANs in the list are monitored on trunk ports or on voice VLAN access ports.
- SPAN traffic coming from other port types is not affected by VLAN filtering; that is, all VLANs are allowed on other ports.
- VLAN filtering affects only traffic forwarded to the destination SPAN port and does not affect the switching of normal traffic.

Destination Port

Each local SPAN session or RSPAN destination session must have a destination port (also called a monitoring port) that receives a copy of traffic from the source ports or VLANs and sends the SPAN packets to the user, usually a network analyzer.

A destination port has these characteristics:

- For a local SPAN session, the destination port must reside on the same switch or switch stack as the source port. For an RSPAN session, it is located on the switch containing the RSPAN destination session. There is no destination port on a switch or switch stack running only an RSPAN source session.
- When a port is configured as a SPAN destination port, the configuration overwrites the original port configuration. When the SPAN destination configuration is removed, the port reverts to its previous configuration. If a configuration change is made to the port while it is acting as a SPAN destination port, the change does not take effect until the SPAN destination configuration had been removed.

Note When QoS is configured on the SPAN destination port, QoS takes effect immediately.

- If the port was in an EtherChannel group, it is removed from the group while it is a destination port. If it was a routed port, it is no longer a routed port.
- It can be any Ethernet physical port.
- It cannot be a secure port.
- It cannot be a source port.
- It can be an EtherChannel group (**ON** mode only).
- It cannot be a VLAN.
- It can participate in only one SPAN session at a time (a destination port in one SPAN session cannot be a destination port for a second SPAN session).
- When it is active, incoming traffic is disabled. The port does not transmit any traffic except that required for the SPAN session. Incoming traffic is never learned or forwarded on a destination port.
- If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.
- It does not participate in any of the Layer 2 protocols (STP, VTP, CDP, DTP, PagP).

- A destination port that belongs to a source VLAN of any SPAN session is excluded from the source list and is not monitored.
- The maximum number of destination ports in a switch or switch stack is 64.

Local SPAN and RSPAN destination ports function differently with VLAN tagging and encapsulation:

- For local SPAN, if the **encapsulation replicate** keywords are specified for the destination port, these packets appear with the original encapsulation (untagged, ISL, or IEEE 802.1Q). If these keywords are not specified, packets appear in the untagged format. Therefore, the output of a local SPAN session with **encapsulation replicate** enabled can contain a mixture of untagged, ISL, or IEEE 802.1Q-tagged packets.
- For RSPAN, the original VLAN ID is lost because it is overwritten by the RSPAN VLAN identification. Therefore, all packets appear on the destination port as untagged.

RSPAN VLAN

The RSPAN VLAN carries SPAN traffic between RSPAN source and destination sessions. RSPAN VLAN has these special characteristics:

- All traffic in the RSPAN VLAN is always flooded.
- No MAC address learning occurs on the RSPAN VLAN.
- RSPAN VLAN traffic only flows on trunk ports.
- RSPAN VLANs must be configured in VLAN configuration mode by using the **remote-span** VLAN configuration mode command.
- STP can run on RSPAN VLAN trunks but not on SPAN destination ports.
- An RSPAN VLAN cannot be a private-VLAN primary or secondary VLAN.

For VLANs 1 to 1005 that are visible to VLAN Trunking Protocol (VTP), the VLAN ID and its associated RSPAN characteristic are propagated by VTP. If you assign an RSPAN VLAN ID in the extended VLAN range (1006 to 4094), you must manually configure all intermediate switches.

It is normal to have multiple RSPAN VLANs in a network at the same time with each RSPAN VLAN defining a network-wide RSPAN session. That is, multiple RSPAN source sessions anywhere in the network can contribute packets to the RSPAN session. It is also possible to have multiple RSPAN destination sessions throughout the network, monitoring the same RSPAN VLAN and presenting traffic to the user. The RSPAN VLAN ID separates the sessions.

SPAN and RSPAN Interaction with Other Features

SPAN interacts with these features:

- Routing—SPAN does not monitor routed traffic. VSPAN only monitors traffic that enters or exits the switch, not traffic that is routed between VLANs. For example, if a VLAN is being Rx-monitored and the switch routes traffic from another VLAN to the monitored VLAN, that traffic is not monitored and not received on the SPAN destination port.
- STP—A destination port does not participate in STP while its SPAN or RSPAN session is active. The destination port can participate in STP after the SPAN or RSPAN session is disabled. On a source port, SPAN does not affect the STP status. STP can be active on trunk ports carrying an RSPAN VLAN.

- CDP—A SPAN destination port does not participate in CDP while the SPAN session is active. After the SPAN session is disabled, the port again participates in CDP.
- VTP—You can use VTP to prune an RSPAN VLAN between switches.
- VLAN and trunking—You can modify VLAN membership or trunk settings for source or destination ports at any time. However, changes in VLAN membership or trunk settings for a destination port do not take effect until you remove the SPAN destination configuration. Changes in VLAN membership or trunk settings for a source port immediately take effect, and the respective SPAN sessions automatically adjust accordingly.
- EtherChannel—You can configure an EtherChannel group as a source port or a SPAN destination port. When a group is configured as a SPAN source, the entire group is monitored.

  If a physical port is added to a monitored EtherChannel group, the new port is added to the SPAN source port list. If a port is removed from a monitored EtherChannel group, it is automatically removed from the source port list.

  A physical port that belongs to an EtherChannel group can be configured as a SPAN source port and still be a part of the EtherChannel. In this case, data from the physical port is monitored as it participates in the EtherChannel. However, if a physical port that belongs to an EtherChannel group is configured as a SPAN destination, it is removed from the group. After the port is removed from the SPAN session, it rejoins the EtherChannel group. Ports removed from an EtherChannel group remain members of the group, but they are in the inactive or suspended state.

  If a physical port that belongs to an EtherChannel group is a destination port and the EtherChannel group is a source, the port is removed from the EtherChannel group and from the list of monitored ports.
- Multicast traffic can be monitored. For egress and ingress port monitoring, only a single unedited packet is sent to the SPAN destination port. It does not reflect the number of times the multicast packet is sent.
- A private-VLAN port cannot be a SPAN destination port.
- A secure port cannot be a SPAN destination port.

  For SPAN sessions, do not enable port security on ports with monitored egress when ingress forwarding is enabled on the destination port. For RSPAN source sessions, do not enable port security on any ports with monitored egress.
- An IEEE 802.1x port can be a SPAN source port. You can enable IEEE 802.1x on a port that is a SPAN destination port; however, IEEE 802.1x is disabled until the port is removed as a SPAN destination.

  For SPAN sessions, do not enable IEEE 802.1x on ports with monitored egress when ingress forwarding is enabled on the destination port. For RSPAN source sessions, do not enable IEEE 802.1x on any ports that are egress monitored.

SPAN and RSPAN and Device Stacks

Because the stack of switches represents one logical switch, local SPAN source ports and destination ports can be in different switches in the stack. Therefore, the addition or deletion of switches in the stack can affect a local SPAN session, as well as an RSPAN source or destination session. An active session can become inactive when a switch is removed from the stack or an inactive session can become active when a switch is added to the stack.

Flow-Based SPAN

You can control the type of network traffic to be monitored in SPAN or RSPAN sessions by using flow-based SPAN (FSPAN) or flow-based RSPAN (FRSPAN), which apply access control lists (ACLs) to the monitored traffic on the source ports. The FSPAN ACLs can be configured to filter IPv4, IPv6, and non-IP monitored traffic.

You apply an ACL to a SPAN session through the interface. It is applied to all the traffic that is monitored on all interfaces in the SPAN session.The packets that are permitted by this ACL are copied to the SPAN destination port. No other packets are copied to the SPAN destination port.

The original traffic continues to be forwarded, and any port, VLAN, and router ACLs attached are applied. The FSPAN ACL does not have any effect on the forwarding decisions. Similarly, the port, VLAN, and router ACLs do not have any effect on the traffic monitoring. If a security input ACL denies a packet and it is not forwarded, the packet is still copied to the SPAN destination ports if the FSPAN ACL permits it. But if the security output ACL denies a packet and it is not sent, it is not copied to the SPAN destination ports. However, if the security output ACL permits the packet to go out, it is only copied to the SPAN destination ports if the FSPAN ACL permits it. This is also true for an RSPAN session.

You can attach three types of FSPAN ACLs to the SPAN session:

- IPv4 FSPAN ACL— Filters only IPv4 packets.
- IPv6 FSPAN ACL— Filters only IPv6 packets.
- MAC FSPAN ACL— Filters only non-IP packets.

If a VLAN-based FSPAN session configured on a stack cannot fit in the hardware memory on one or more switches, it is treated as unloaded on those switches, and traffic meant for the FSPAN ACL and sourcing on that switch is not copied to the SPAN destination ports. The FSPAN ACL continues to be correctly applied, and traffic is copied to the SPAN destination ports on the switches where the FSPAN ACL fits in the hardware memory.

When an empty FSPAN ACL is attached, some hardware functions copy all traffic to the SPAN destination ports for that ACL. If sufficient hardware resources are not available, even an empty FSPAN ACL can be unloaded.

IPv4 and MAC FSPAN ACLs are supported on all feature sets. IPv6 FSPAN ACLs are supported only in the advanced IP Services feature set.

Default SPAN and RSPAN Configuration

Table 32: Default SPAN and RSPAN Configuration

Feature	Default Setting
SPAN state (SPAN and RSPAN)	Disabled.
Source port traffic to monitor	Both received and sent traffic (**both**).
Encapsulation type (destination port)	Native form (untagged packets).
Ingress forwarding (destination port)	Disabled.

Feature	Default Setting
VLAN filtering	On a trunk interface used as a source port, all VLANs are monitored.
RSPAN VLANs	None configured.

Configuration Guidelines

SPAN Configuration Guidelines

- To remove a source or destination port or VLAN from the SPAN session, use the **no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} global configuration command or the **no monitor session** *session_number* **destination interface** *interface-id* global configuration command. For destination interfaces, the **encapsulation** options are ignored with the **no** form of the command.
- To monitor all VLANs on the trunk port, use the **no monitor session** *session_number* **filter** global configuration command.

RSPAN Configuration Guidelines

- All the SPAN configuration guidelines apply to RSPAN.
- As RSPAN VLANs have special properties, you should reserve a few VLANs across your network for use as RSPAN VLANs; do not assign access ports to these VLANs.
- You can apply an output ACL to RSPAN traffic to selectively filter or monitor specific packets. Specify these ACLs on the RSPAN VLAN in the RSPAN source switches.
- For RSPAN configuration, you can distribute the source ports and the destination ports across multiple switches in your network.
- Access ports (including voice VLAN ports) on the RSPAN VLAN are put in the inactive state.
- You can configure any VLAN as an RSPAN VLAN as long as these conditions are met:
  - The same RSPAN VLAN is used for an RSPAN session in all the switches.
  - All participating switches support RSPAN.

FSPAN and FRSPAN Configuration Guidelines

- FSPAN is not supported on LAN base.
- When at least one FSPAN ACL is attached, FSPAN is enabled.
- When you attach at least one FSPAN ACL that is not empty to a SPAN session, and you have not attached one or more of the other FSPAN ACLs (for instance, you have attached an IPv4 ACL that is not empty, and have not attached IPv6 and MAC ACLs), FSPAN blocks the traffic that would have been filtered by the unattached ACLs. Therefore, this traffic is not monitored.

How to Configure SPAN and RSPAN

Creating a Local SPAN Session

Follow these steps to create a SPAN session and specify the source (monitored) ports or VLANs and the destination (monitoring) ports.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} **Example:** `Switch(config)# no monitor session all`	Removes any existing SPAN configuration for the session. • For *session_number*, the range is 1 to 66. • **all**—Removes all SPAN sessions. • **local**—Removes all local sessions. • **remote**—Removes all remote SPAN sessions.
Step 4	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] **Example:** `Switch(config)# monitor session 1 source interface gigabitethernet1/0/1`	Specifies the SPAN session and the source port (monitored port). • For *session_number*, the range is 1 to 66. • For *interface-id*, specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). Valid port-channel numbers are 1 to 48. • For *vlan-id*, specify the source VLAN to monitor. The range is 1 to 4094 (excluding the RSPAN VLAN).

	Command or Action	Purpose
		Note A single session can include multiple sources (ports or VLANs) defined in a series of commands, but you cannot combine source ports and source VLANs in one session. • (Optional) [**,** | **-**] Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen. • (Optional) **both** | **rx** | **tx**—Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic. • **both**—Monitors both received and sent traffic. • **rx**—Monitors received traffic. • **tx**—Monitors sent traffic. **Note** You can use the **monitor session** *session_number* **source** command multiple times to configure multiple source ports.
Step 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**]} **Example:** `Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2 encapsulation replicate`	Specifies the SPAN session and the destination port (monitoring port). The port LED changes to amber when the configuration changes take effect. The LED returns to its original state(green) only after removing the SPAN destination configuration. **Note** For local SPAN, you must use the same session number for the source and destination interfaces. • For *session_number*, specify the session number entered in step 4. • For *interface-id*, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN. • (Optional) [**,** | **-**] Specifies a series or range of interfaces. Enter a space before and after

	Command or Action	Purpose
		the comma; enter a space before and after the hyphen. (Optional) **encapsulation replicate** specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged). **Note** You can use **monitor session** *session_number* **destination** command multiple times to configure multiple destination ports.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Creating a Local SPAN Session and Configuring Incoming Traffic

Follow these steps to create a SPAN session, to specify the source ports or VLANs and the destination ports, and to enable incoming traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} **Example:** `Switch(config)# no monitor session all`	Removes any existing SPAN configuration for the session. • For *session_number*, the range is 1 to 66. • **all**—Removes all SPAN sessions. • **local**—Removes all local sessions. • **remote**—Removes all remote SPAN sessions.
Step 4	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] **Example:** `Switch(config)# monitor session 2 source gigabitethernet1/0/1 rx`	Specifies the SPAN session and the source port (monitored port).
Step 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**] [**ingress** {**dot1q vlan** *vlan-id* | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]} **Example:** `Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate ingress dot1q vlan 6`	Specifies the SPAN session, the destination port, the packet encapsulation, and the ingress VLAN and encapsulation. • For *session_number*, specify the session number entered in Step 4. • For *interface-id*, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN. • (Optional) [**,** | **-**]—Specifies a series or range of interfaces. Enter a space before and after the comma or hyphen. • (Optional) **encapsulation replicate** specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged). • **ingress** enables forwarding of incoming traffic on the destination port and to specify the encapsulation type:

	Command or Action	Purpose
		• **dot1q vlan** *vlan-id*—Accepts incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN. • **untagged vlan** *vlan-id* or **vlan** *vlan-id*—Accepts incoming packets with untagged encapsulation type with the specified VLAN as the default VLAN.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Specifying VLANs to Filter

Follow these steps to limit SPAN source traffic to specific VLANs.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters the global configuration mode.

	Command or Action	Purpose
	`Switch# configure terminal`	
Step 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} **Example:** `Switch(config)# no monitor session all`	Removes any existing SPAN configuration for the session. • For *session_number*, the range is 1 to 66. • **all**—Removes all SPAN sessions. • **local**—Removes all local sessions. • **remote**—Removes all remote SPAN sessions.
Step 4	**monitor session** *session_number* **source interface** *interface-id* **Example:** `Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx`	Specifies the characteristics of the source port (monitored port) and SPAN session. • For *session_number*, the range is 1 to 66. • For *interface-id*, specify the source port to monitor. The interface specified must already be configured as a trunk port.
Step 5	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**] **Example:** `Switch(config)# monitor session 2 filter vlan 1 - 5 , 9`	Limits the SPAN source traffic to specific VLANs. • For *session_number*, enter the session number specified in Step 4. • For *vlan-id*, the range is 1 to 4094. • (Optional) Use a comma (**,**) to specify a series of VLANs, or use a hyphen (**-**) to specify a range of VLANs. Enter a space before and after the comma; enter a space before and after the hyphen.
Step 6	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**]} **Example:** `Switch(config)# monitor session 2 destination interface gigabitethernet1/0/1`	Specifies the SPAN session and the destination port (monitoring port). • For *session_number*, specify the session number entered in Step 4. • For *interface-id*, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN. • (Optional) [**,** | **-**] Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.

	Command or Action	Purpose
		• (Optional) **encapsulation replicate** specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged).
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 8	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 9	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring a VLAN as an RSPAN VLAN

Follow these steps to create a new VLAN, then configure it to be the RSPAN VLAN for the RSPAN session.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**vlan** *vlan-id* **Example:**	Enters a VLAN ID to create a VLAN, or enters the VLAN ID of an existing VLAN, and enters

	Command or Action	Purpose
	`Switch(config)# vlan 100`	VLAN configuration mode. The range is 2 to 1001 and 1006 to 4094. The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 through 1005 (reserved for Token Ring and FDDI VLANs).
Step 4	**remote-span** **Example:** `Switch(config-vlan)# remote-span`	Configures the VLAN as an RSPAN VLAN.
Step 5	**end** **Example:** `Switch(config-vlan)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

You must create the RSPAN VLAN in all switches that will participate in RSPAN. If the RSPAN VLAN-ID is in the normal range (lower than 1005) and VTP is enabled in the network, you can create the RSPAN VLAN in one switch, and VTP propagates it to the other switches in the VTP domain. For extended-range VLANs (greater than 1005), you must configure RSPAN VLAN on both source and destination switches and any intermediate switches.

Use VTP pruning to get an efficient flow of RSPAN traffic, or manually delete the RSPAN VLAN from all trunks that do not need to carry the RSPAN traffic.

To remove the remote SPAN characteristic from a VLAN and convert it back to a normal VLAN, use the **no remote-span** VLAN configuration command.

To remove a source port or VLAN from the SPAN session, use the **no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} global configuration command. To remove the RSPAN VLAN from the session, use the **no monitor session** *session_number* **destination remote vlan** *vlan-id*.

Creating an RSPAN Source Session

Follow these steps to create and start an RSPAN source session and to specify the monitored source and the destination RSPAN VLAN.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} **Example:** `Switch(config)# no monitor session 1`	Removes any existing SPAN configuration for the session. • For *session_number*, the range is 1 to 66. • **all**—Removes all SPAN sessions. • **local**—Removes all local sessions. • **remote**—Removes all remote SPAN sessions.
Step 4	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] **Example:** `Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 tx`	Specifies the RSPAN session and the source port (monitored port). • For *session_number*, the range is 1 to 66. • Enter a source port or source VLAN for the RSPAN session: • For *interface-id*, specifies the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). Valid port-channel numbers are 1 to 48. • For *vlan-id*, specifies the source VLAN to monitor. The range is 1 to 4094 (excluding the RSPAN VLAN). A single session can include multiple sources (ports or VLANs), defined in

	Command or Action	Purpose
		a series of commands, but you cannot combine source ports and source VLANs in one session. • (Optional) [**,** | **-**]—Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen. • (Optional) **both** | **rx** | **tx**—Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic. • **both**—Monitors both received and sent traffic. • **rx**—Monitors received traffic. • **tx**—Monitors sent traffic.
Step 5	**monitor session** *session_number* **destination remote vlan** *vlan-id* **Example:** `Switch(config)# monitor session 1 destination remote vlan 100`	Specifies the RSPAN session, the destination RSPAN VLAN, and the destination-port group. • For *session_number*, enter the number defined in Step 4. • For *vlan-id*, specify the source RSPAN VLAN to monitor.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Specifying VLANs to Filter

Follow these steps to configure the RSPAN source session to limit RSPAN source traffic to specific VLANs.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} **Example:** `Switch(config)# no monitor session 2`	Removes any existing SPAN configuration for the session. • For *session_number*, the range is 1 to 66. • **all**—Removes all SPAN sessions. • **local**—Removes all local sessions. • **remote**—Removes all remote SPAN sessions.
Step 4	**monitor session** *session_number* **source interface** *interface-id* **Example:** `Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx`	Specifies the characteristics of the source port (monitored port) and SPAN session. • For *session_number*, the range is 1 to 66. • For *interface-id*, specify the source port to monitor. The interface specified must already be configured as a trunk port.
Step 5	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**] **Example:** `Switch(config)# monitor session 2 filter vlan 1 - 5 , 9`	Limits the SPAN source traffic to specific VLANs. • For *session_number*, enter the session number specified in step 4. • For *vlan-id*, the range is 1 to 4094. • (Optional) **,** | **-** Use a comma (**,**) to specify a series of VLANs or use a hyphen (**-**) to specify a range of VLANs. Enter a space before and after the comma; enter a space before and after the hyphen.

	Command or Action	Purpose
Step 6	**monitor session** *session_number* **destination remote vlan** *vlan-id* **Example:** `Switch(config)# monitor session 2 destination remote vlan 902`	Specifies the RSPAN session and the destination remote VLAN (RSPAN VLAN). • For *session_number*, enter the session number specified in Step 4. • For *vlan-id*, specify the RSPAN VLAN to carry the monitored traffic to the destination port.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 8	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 9	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Creating an RSPAN Destination Session

You configure an RSPAN destination session on a different switch or switch stack; that is, not the switch or switch stack on which the source session was configured.

Follow these steps to define the RSPAN VLAN on that switch, to create an RSPAN destination session, and to specify the source RSPAN VLAN and the destination port.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters the global configuration mode.

	Command or Action	Purpose
	`Switch# configure terminal`	
Step 3	**vlan** *vlan-id* **Example:** `Switch(config)# vlan 901`	Specifies the VLAN ID of the RSPAN VLAN created from the source switch, and enters VLAN configuration mode. If both switches are participating in VTP and the RSPAN VLAN ID is from 2 to 1005, Steps 3 through 5 are not required because the RSPAN VLAN ID is propagated through the VTP network.
Step 4	**remote-span** **Example:** `Switch(config-vlan)# remote-span`	Identifies the VLAN as the RSPAN VLAN.
Step 5	**exit** **Example:** `Switch(config-vlan)# exit`	Returns to global configuration mode.
Step 6	**no monitor session** {*session_number* | **all** | **local** | **remote**} **Example:** `Switch(config)# no monitor session 1`	Removes any existing SPAN configuration for the session. • For *session_number*, the range is 1 to 66. • **all**—Removes all SPAN sessions. • **local**—Removes all local sessions. • **remote**—Removes all remote SPAN sessions.
Step 7	**monitor session** *session_number* **source remote vlan** *vlan-id* **Example:** `Switch(config)# monitor session 1 source remote vlan 901`	Specifies the RSPAN session and the source RSPAN VLAN. • For *session_number*, the range is 1 to 66. • For *vlan-id*, specify the source RSPAN VLAN to monitor.
Step 8	**monitor session** *session_number* **destination interface** *interface-id* **Example:** `Switch(config)# monitor session 1 destination interface gigabitethernet2/0/1`	Specifies the RSPAN session and the destination interface. • For *session_number*, enter the number defined in Step 7. In an RSPAN destination session, you must use the same session number for the source RSPAN VLAN and the destination port.

	Command or Action	Purpose
		• For *interface-id*, specify the destination interface. The destination interface must be a physical interface. • Though visible in the command-line help string, **encapsulation replicate** is not supported for RSPAN. The original VLAN ID is overwritten by the RSPAN VLAN ID, and all packets appear on the destination port as untagged.
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 10	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 11	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Creating an RSPAN Destination Session and Configuring Incoming Traffic

Follow these steps to create an RSPAN destination session, to specify the source RSPAN VLAN and the destination port, and to enable incoming traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters the global configuration mode.

	Command or Action	Purpose
	`Switch# configure terminal`	
Step 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} **Example:** `Switch(config)# no monitor session 2`	Removes any existing SPAN configuration for the session. • For *session_number*, the range is 1 to 66. • **all**—Removes all SPAN sessions. • **local**—Removes all local sessions. • **remote**—Removes all remote SPAN sessions.
Step 4	**monitor session** *session_number* **source remote vlan** *vlan-id* **Example:** `Switch(config)# monitor session 2 source remote vlan 901`	Specifies the RSPAN session and the source RSPAN VLAN. • For *session_number*, the range is 1 to 66. • For *vlan-id*, specify the source RSPAN VLAN to monitor.
Step 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**ingress** {**dot1q vlan** *vlan-id* | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]} **Example:** `Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress vlan 6`	Specifies the SPAN session, the destination port, the packet encapsulation, and the incoming VLAN and encapsulation. • For *session_number*, enter the number defined in Step 5. In an RSPAN destination session, you must use the same session number for the source RSPAN VLAN and the destination port. • For *interface-id*, specify the destination interface. The destination interface must be a physical interface. • Though visible in the command-line help string, **encapsulation replicate** is not supported for RSPAN. The original VLAN ID is overwritten by the RSPAN VLAN ID, and all packets appear on the destination port as untagged. • (Optional) [**,** | **-**] Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen. • Enter **ingress** with additional keywords to enable forwarding of incoming traffic on

	Command or Action	Purpose
		the destination port and to specify the encapsulation type: • **dot1q vlan** *vlan-id*—Forwards incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN. • **untagged vlan** *vlan-id* or **vlan** *vlan-id*—Forwards incoming packets with untagged encapsulation type with the specified VLAN as the default VLAN.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring an FSPAN Session

Follow these steps to create a SPAN session, specify the source (monitored) ports or VLANs and the destination (monitoring) ports, and configure FSPAN for the session.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} **Example:** `Switch(config)# no monitor session 2`	Removes any existing SPAN configuration for the session. • For *session_number*, the range is 1 to 66. • **all**—Removes all SPAN sessions. • **local**—Removes all local sessions. • **remote**—Removes all remote SPAN sessions.
Step 4	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] **Example:** `Switch(config)# monitor session 2 source interface gigabitethernet1/0/1`	Specifies the SPAN session and the source port (monitored port). • For *session_number*, the range is 1 to 66. • For *interface-id*, specifies the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). Valid port-channel numbers are 1 to 48. • For *vlan-id*, specify the source VLAN to monitor. The range is 1 to 4094 (excluding the RSPAN VLAN). **Note** A single session can include multiple sources (ports or VLANs) defined in a series of commands, but you cannot combine source ports and source VLANs in one session. • (Optional) [**,** | **-**]—Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen. • (Optional) [**both** | **rx** | **tx**]—Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the SPAN monitors both sent and received traffic. • **both**—Monitors both sent and received traffic. This is the default.

	Command or Action	Purpose
		• **rx**—Monitors received traffic. • **tx**—Monitors sent traffic. **Note** You can use the **monitor session** *session_number* **source** command multiple times to configure multiple source ports.
Step 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**]} **Example:** `Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate`	Specifies the SPAN session and the destination port (monitoring port). • For *session_number*, specify the session number entered in Step 4. • For **destination**, specify the following parameters: • For *interface-id*, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN. • (Optional) [**,** | **-**] Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen. • (Optional) **encapsulation replicate** specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged). **Note** For local SPAN, you must use the same session number for the source and destination interfaces. You can use **monitor session** *session_number* **destination** command multiple times to configure multiple destination ports.
Step 6	**monitor session** *session_number* **filter** {**ip** | **ipv6** | **mac**} **access-group** {*access-list-number* | *name*} **Example:**	Specifies the SPAN session, the types of packets to filter, and the ACLs to use in an FSPAN session. • For *session_number*, specify the session number entered in Step 4.

	Command or Action	Purpose
	`Switch(config)# monitor session 2 filter ipv6 access-group 4`	• For *access-list-number*, specify the ACL number that you want to use to filter traffic. • For *name*, specify the ACL name that you want to use to filter traffic.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 8	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 9	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring an FRSPAN Session

Follow these steps to start an RSPAN source session, specify the monitored source and the destination RSPAN VLAN, and configure FRSPAN for the session.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} **Example:**	Removes any existing SPAN configuration for the session. • For *session_number*, the range is 1 to 66.

	Command or Action	Purpose
	`Switch(config)# no monitor session 2`	• **all**—Removes all SPAN sessions. • **local**—Removes all local sessions. • **remote**—Removes all remote SPAN sessions.
Step 4	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] **Example:** `Switch(config)# monitor session 2 source interface gigabitethernet1/0/1`	Specifies the SPAN session and the source port (monitored port). • For *session_number*, the range is 1 to 66. • For *interface-id*, specifies the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). Valid port-channel numbers are 1 to 48. • For *vlan-id*, specify the source VLAN to monitor. The range is 1 to 4094 (excluding the RSPAN VLAN). **Note** A single session can include multiple sources (ports or VLANs) defined in a series of commands, but you cannot combine source ports and source VLANs in one session. • (Optional) [**,** | **-**]—Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen. • (Optional) [**both** | **rx** | **tx**]—Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the SPAN monitors both sent and received traffic. • **both**—Monitors both sent and received traffic. This is the default. • **rx**—Monitors received traffic. • **tx**—Monitors sent traffic. **Note** You can use the **monitor session** *session_number* **source** command multiple times to configure multiple source ports.

	Command or Action	Purpose
Step 5	**monitor session** *session_number* **destination remote vlan** *vlan-id* **Example:** `Switch(config)# monitor session 2 destination remote vlan 5`	Specifies the RSPAN session and the destination RSPAN VLAN. • For *session_number*, enter the number defined in Step 4. • For *vlan-id*, specify the destination RSPAN VLAN to monitor.
Step 6	**vlan** *vlan-id* **Example:** `Switch(config)# vlan 10`	Enters the VLAN configuration mode. For *vlan-id*, specify the source RSPAN VLAN to monitor.
Step 7	**remote-span** **Example:** `Switch(config-vlan)# remote-span`	Specifies that the VLAN you specified in Step 5 is part of the RSPAN VLAN.
Step 8	**exit** **Example:** `Switch(config-vlan)# exit`	Returns to global configuration mode.
Step 9	**monitor session** *session_number* **filter** {**ip** | **ipv6** | **mac**} **access-group** {*access-list-number* | *name*} **Example:** `Switch(config)# monitor session 2 filter ip access-group 7`	Specifies the RSPAN session, the types of packets to filter, and the ACLs to use in an FRSPAN session. • For *session_number*, specify the session number entered in Step 4. • For *access-list-number*, specify the ACL number that you want to use to filter traffic. • For *name*, specify the ACL name that you want to use to filter traffic.
Step 10	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 11	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.

	Command or Action	Purpose
Step 12	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Monitoring SPAN and RSPAN Operations

The following table describes the command used to display SPAN and RSPAN operations configuration and results to monitor operations:

Table 33: Monitoring SPAN and RSPAN Operations

Command	Purpose
show monitor	Displays the current SPAN, RSPAN, FSPAN, or FRSPAN configuration.

SPAN and RSPAN Configuration Examples

Example: Configuring Local SPAN

This example shows how to set up SPAN session 1 for monitoring source port traffic to a destination port. First, any existing SPAN configuration for session 1 is deleted, and then bidirectional traffic is mirrored from source Gigabit Ethernet port 1 to destination Gigabit Ethernet port 2, retaining the encapsulation method.

```
Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
encapsulation replicate
Switch(config)# end
```

This example shows how to remove port 1 as a SPAN source for SPAN session 1:

```
Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# end
```

This example shows how to disable received traffic monitoring on port 1, which was configured for bidirectional monitoring:

```
Switch> enable
```

```
Switch# configure terminal
Switch(config)# no monitor session 1 source interface gigabitethernet1/0/1 rx
```

The monitoring of traffic received on port 1 is disabled, but traffic sent from this port continues to be monitored.

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor received traffic on all ports belonging to VLANs 1 through 3, and send it to destination Gigabit Ethernet port 2. The configuration is then modified to also monitor all traffic on all ports belonging to VLAN 10.

```
Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2
Switch(config)# monitor session 2 source vlan 10
Switch(config)# end
```

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor received traffic on Gigabit Ethernet source port 1, and send it to destination Gigabit Ethernet port 2 with the same egress encapsulation type as the source port, and to enable ingress forwarding with IEEE 802.1Q encapsulation and VLAN 6 as the default ingress VLAN:

```
Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source gigabitethernet1/0/1 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
 replicate ingress dot1q vlan 6
Switch(config)# end
```

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor traffic received on Gigabit Ethernet trunk port 2, and send traffic for only VLANs 1 through 5 and VLAN 9 to destination Gigabit Ethernet port 1:

```
Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/1
Switch(config)# end
```

Examples: Creating an RSPAN VLAN

This example shows how to create the RSPAN VLAN 901:

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 901
Switch(config-vlan)# remote span
Switch(config-vlan)# end
```

This example shows how to remove any existing RSPAN configuration for session 1, configure RSPAN session 1 to monitor multiple source interfaces, and configure the destination as RSPAN VLAN 901:

```
Switch> enable
```

```
Switch# configure terminal
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 tx
Switch(config)# monitor session 1 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 1 source interface port-channel 2
Switch(config)# monitor session 1 destination remote vlan 901
Switch(config)# end
```

This example shows how to remove any existing configuration on RSPAN session 2, configure RSPAN session 2 to monitor traffic received on trunk port 2, and send traffic for only VLANs 1 through 5 and 9 to destination RSPAN VLAN 902:

```
Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination remote vlan 902
Switch(config)# end
```

This example shows how to configure VLAN 901 as the source remote VLAN and port 1 as the destination interface:

```
Switch> enable
Switch# configure terminal
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface gigabitethernet2/0/1
Switch(config)# end
```

This example shows how to configure VLAN 901 as the source remote VLAN in RSPAN session 2, to configure Gigabit Ethernet source port 2 as the destination interface, and to enable forwarding of incoming traffic on the interface with VLAN 6 as the default receiving VLAN:

```
Switch> enable
Switch# configure terminal
Switch(config)# monitor session 2 source remote vlan 901
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress vlan 6
Switch(config)# end
```

Additional References

Related Documents

Related Topic	Document Title
System Commands	*Network Management Command Reference, Cisco IOS XE Release 3E*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
None	-

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

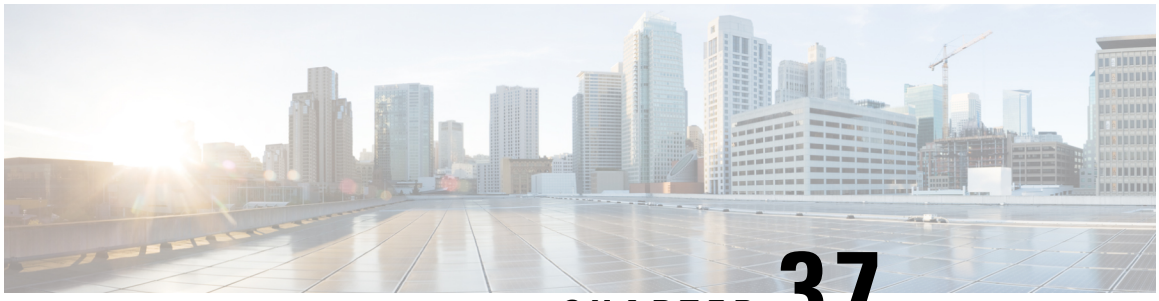
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for SPAN and RSPAN

Release	Modification
Cisco IOS XE 3.2SE	Switch Port Analyzer (SPAN): Allows monitoring of switch traffic on a port or VLAN using a sniffer/analyzer or RMON probe. This feature was introduced.
Cisco IOS XE 3.2SE	Flow-based Switch Port Analyzer (SPAN): Provides a method to capture only required data between end hosts by using specified filters. The filters are defined in terms of access lists that limit IPv4, IPv6 or IPv4 + IPv6, or non-IP traffic (MAC) between specified source and destination addresses. This feature was introduced.

Release	Modification
Cisco IOS XE 3.2SE	SPAN destination port support on EtherChannels: Provides the ability to configure a SPAN destination port on an EtherChannel. This feature was introduced.
Cisco IOS XE 3.2SE	Switch Port Analyzer (SPAN) - distributed egress SPAN: Provides distributed egress SPAN functionality onto line cards in conjunction with ingress SPAN already been distributed to line cards. By distributing egress SPAN functionalities onto line cards, the performance of the system is improved. This feature was introduced.



CHAPTER 37

Configuring Wireshark

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Wireshark

- Wireshark is supported on Supervisor Engine 7-E, Supervisor Engine 7L-E, Catalyst 3850, Catalyst 3650, Wireless LAN Controller 5700 Series, Catalyst 4500X-16, and Catalyst 4500X-32.
- IP Base image or IP Services image is required for Embedded Wireshark.

Restrictions for Wireshark

- Starting in Cisco IOS Release XE 3.3.0(SE), global packet capture on Wireshark is not supported.
- Capture filters are not supported.

- The CLI for configuring Wireshark requires that the feature be executed only from EXEC mode. Actions that usually occur in configuration submode (such as defining capture points), are handled at the EXEC mode instead. All key commands are not NVGEN'd and are not synchronized to the standby supervisor in NSF and SSO scenarios.
- Packets captured in the output direction of an interface might not reflect the changes made by switch rewrite (includes TTL, VLAN tag, CoS, checksum, MAC addresses, DSCP, precedent, UP, etc.).
- Limiting circular file storage by file size is not supported.

Wireless Packet Capture

- The only form of wireless capture is a CAPWAP tunnel capture.
- When capturing CAPWAP tunnels, no other interface types can be used as attachment points on the same capture point.
- Capturing multiple CAPWAP tunnels is supported.
- Core filters are not applied and should be omitted when capturing a CAPWAP tunnel.
- To capture a CAPWAP data tunnel, each CAPWAP tunnel is mapped to a physical port and an appropriate ACL will be applied to filter the traffic.
- To capture a CAPWAP non-data tunnel, the switch is set to capture traffic on all ports and apply an appropriate ACL to filter the traffic.
- To capture a CAPWAP tunnel, no matter what kind, the controller will be told to capture the traffic on all physical ports and apply an appropriate ACL to filter the traffic.

Configuration Limitations

- Starting from Cisco IOS release 16.1, as many as 8 capture points can be defined, but only one can be active at a time. You must stop one before you can start the other.
- You cannot use VRFs, management ports, and private VLANs as attachment points.
- Only one ACL (IPv4, IPv6 or MAC) is allowed in a Wireshark class map.
- Wireshark cannot capture packets on a destination SPAN port.
- Wireshark stops capturing packets when one of the attachment points (interfaces) attached to a capture point stops working. For example, if the device that is associated with an attachment point is unplugged from the switch. To resume capturing packets, restart manually.
- CPU-injected packets are considered control plane packets and are not captured on an interface egress capture.
- MAC ACL is only used for non-IP packets such as ARP. It will not be supported on a Layer 3 port or SVI.
- IPv6-based ACLs are not supported in VACL.
- Layer 2 EtherChannels are not supported. Individual members like GigabitEthernet 1 and GigabitEthernet 2 are supported on Layer 3 EtherChannels.

- ACL logging and Wireshark are incompatible. After Wireshark is activated, it takes priority. All traffic, including traffic captured by ACL logging on ports, will be redirected to Wireshark. We recommend that you deactivate ACL logging before you start Wireshark. Otherwise, Wireshark traffic is contaminated by ACL logging traffic.
- Wireshark does not capture packets dropped by floodblock.
- If you capture both PACL and RACL on the same port, only one copy is sent to the CPU. If you capture a DTLS-encrypted CAPWAP interface, two copies are sent to Wireshark, one encrypted and the other decrypted. The same behavior will occur if we capture a Layer 2 interface carrying DTLS-encrypted CAPWAP traffic. The core filter is based on the outer CAPWAP header.
- Control plane packets are not rate limited and do not impact performance. Use filters to limit control plane packet capture.

Information About Wireshark

Wireshark Overview

Wireshark is a packet analyzer program, formerly known as Ethereal, that supports multiple protocols and presents information in a text-based user interface.

The ability to capture and analyze traffic provides data on network activity. Prior to Cisco IOS Release XE 3.3.0(SE), only two features addressed this need: SPAN and debug platform packet. Both have limitations. SPAN is ideal for capturing packets, but can only deliver them by forwarding them to some specified local or remote destination; it provides no local display or analysis support.

So the need exists for a traffic capture and analysis mechanism that is applicable to both hardware and software forwarded traffic and that provides strong packet capture, display, and analysis support, preferably using a well known interface.

Wireshark dumps packets to a file using a well known format called .pcap, and is applied or enabled on individual interfaces. You specify an interface in EXEC mode along with the filter and other parameters. The Wireshark application is applied only when you enter a **start** command, and is removed only when Wireshark stops capturing packets either automatically or manually.

Note The current version of Wireshark installed on the switch is 1.10.8.

Capture Points

A capture point is the central policy definition of the Wireshark feature. The capture point describes all of the characteristics associated with a given instance of Wireshark: which packets to capture, where to capture them from, what to do with the captured packets, and when to stop. Capture points can be modified after creation, and do not become active until explicitly activated with a **start** command. This process is termed activating the capture point or starting the capture point. Capture points are identified by name and can also be manually or automatically deactivated or stopped.

Multiple capture points can be defined, but only one can be active at a time. You need to stop one before you can start the other.

In case of stacked systems, the capture point is activated on the active member. A switchover will terminate any active packet capture session and it will have to be restarted.

Related Topics

Defining a Capture Point, on page 553
Adding or Modifying Capture Point Parameters, on page 558
Deleting Capture Point Parameters, on page 560
Deleting a Capture Point, on page 562
Activating and Deactivating a Capture Point, on page 563
Clearing the Capture Point Buffer, on page 566
Example: Simple Capture and Display, on page 571
Example: Simple Capture and Store, on page 572
Example: Using Buffer Capture, on page 575
Example: Capture Sessions, on page 581
Example: Capture and Store in Lock-step Mode, on page 582
Example: Simple Capture and Store of Packets in Egress Direction, on page 583

Attachment Points

An attachment point is a point in the logical packet process path associated with a capture point. An attachment point is an attribute of the capture point. Packets that impact an attachment point are tested against capture point filters; packets that match are copied and sent to the associated Wireshark instance of the capture point. A specific capture point can be associated with multiple attachment points, with limits on mixing attachment points of different types. Some restrictions apply when you specify attachment points of different types. Attachment points are directional (input or output or both) with the exception of the Layer 2 VLAN attachment point, which is always bidirectional.

In case of stacked systems, the attachment points on all stack members are valid. EPC captures the packets from all the defined attachment points. However these packets are processed only on the active member.

Related Topics

Defining a Capture Point, on page 553
Adding or Modifying Capture Point Parameters, on page 558
Deleting Capture Point Parameters, on page 560
Deleting a Capture Point, on page 562
Activating and Deactivating a Capture Point, on page 563
Clearing the Capture Point Buffer, on page 566
Example: Simple Capture and Display, on page 571
Example: Simple Capture and Store, on page 572
Example: Using Buffer Capture, on page 575
Example: Capture Sessions, on page 581
Example: Capture and Store in Lock-step Mode, on page 582
Example: Simple Capture and Store of Packets in Egress Direction, on page 583

Filters

Filters are attributes of a capture point that identify and limit the subset of traffic traveling through the attachment point of a capture point, which is copied and passed to Wireshark. To be displayed by Wireshark, a packet must pass through an attachment point, as well as all of the filters associated with the capture point.

A capture point has the following types of filters:

- Core system filter—The core system filter is applied by hardware, and its match criteria is limited by hardware. This filter determines whether hardware-forwarded traffic is copied to software for Wireshark purposes.
- Display filter—The display filter is applied by Wireshark. Packets that fail the display filter are not displayed.

Core System Filter

You can specify core system filter match criteria by using the class map or ACL, or explicitly by using the CLI.

Note When specifying CAPWAP as an attachment point, the core system filter is not used.

In some installations, you need to obtain authorization to modify the switch configuration, which can lead to extended delays if the approval process is lengthy. This can limit the ability of network administrators to monitor and analyze traffic. To address this situation, Wireshark supports explicit specification of core system filter match criteria from the EXEC mode CLI. The disadvantage is that the match criteria that you can specify is a limited subset of what class map supports, such as MAC, IP source and destination addresses, ether-type, IP protocol, and TCP/UDP source and destination ports.

If you prefer to use configuration mode, you can define ACLs or have class maps refer capture points to them. Explicit and ACL-based match criteria are used internally to construct class maps and policy maps.

Note The ACL and class map configuration are part of the system and not aspects of the Wireshark feature.

Display Filter

With the display filter, you can direct Wireshark to further narrow the set of packets to display when decoding and displaying from a .pcap file.

Related Topics

Additional References, on page 585

Actions

Wireshark can be invoked on live traffic or on a previously existing .pcap file. When invoked on live traffic, it can perform four types of actions on packets that pass its display filters:

- Captures to buffer in memory to decode and analyze and store
- Stores to a .pcap file
- Decodes and displays

- Stores and displays

When invoked on a .pcap file only, only the decode and display action is applicable.

Storage of Captured Packets to Buffer in Memory

Packets can be stored in the capture buffer in memory for subsequent decode, analysis, or storage to a .pcap file.

The capture buffer can be in linear or circular mode. In linear mode, new packets are discarded when the buffer is full. In circular mode, if the buffer is full, the oldest packets are discarded to accommodate the new packets. Although the buffer can also be cleared when needed, this mode is mainly used for debugging network traffic. However, it is not possible to only clear the contents of the buffer alone without deleting it. Stop the current captures and restart the capture again for this to take effect.

Note If you have more than one capture that is storing packets in a buffer, clear the buffer before starting a new capture to avoid memory loss.

Storage of Captured Packets to a .pcap File

Note When WireShark is used on switches in a stack, packet captures can be stored only on flash or USB flash devices connected to the active switch.

For example, if flash1 is connected to the active switch, and flash2 is connected to the secondary switch, only flash1 can be used to store packet captures.

Attempts to store packet captures on devices other than flash or USB flash devices connected to the active switch will probably result in errors.

Wireshark can store captured packets to a .pcap file. The capture file can be located on the following storage devices:

- Switch on-board flash storage (flash:)
- USB drive (usbflash0:)

Note Attempts to store packet captures on unsupported devices or devices not connected to the active switch will probably result in errors.

When configuring a Wireshark capture point, you can associate a filename. When the capture point is activated, Wireshark creates a file with the specified name and writes packets to it. If the file already exists at the time of creation of the capture point, Wireshark queries you as to whether the file can be overwritten. If the file already exists at the time of activating the capture point, Wireshark will overwrite the existing file. Only one capture point may be associated with a given filename.

If the destination of the Wireshark writing process is full, Wireshark fails with partial data in the file. You must ensure that there is sufficient space in the file system before you start the capture session. With Cisco IOS Release IOS XE 3.3.0(SE), the file system full status is not detected for some storage devices.

You can reduce the required storage space by retaining only a segment, instead of the entire packet. Typically, you do not require details beyond the first 64 or 128 bytes. The default behavior is to store the entire packet.

To avoid possible packet drops when processing and writing to the file system, Wireshark can optionally use a memory buffer to temporarily hold packets as they arrive. Memory buffer size can be specified when the capture point is associated with a .pcap file.

Packet Decoding and Display

Wireshark can decode and display packets to the console. This functionality is possible for capture points applied to live traffic and for capture points applied to a previously existing .pcap file.

Note Decoding and displaying packets may be CPU intensive.

Wireshark can decode and display packet details for a wide variety of packet formats. The details are displayed by entering the **monitor capture name start** command with one of the following keyword options, which place you into a display and decode mode:

- brief—Displays one line per packet (the default).
- detailed—Decodes and displays all the fields of all the packets whose protocols are supported. Detailed modes require more CPU than the other two modes.
- (hexadecimal) dump—Displays one line per packet as a hexadecimal dump of the packet data and the printable characters of each packet.

When you enter the **capture** command with the decode and display option, the Wireshark output is returned to Cisco IOS and displayed on the console unchanged.

Live Traffic Display

Wireshark receives copies of packets from the core system. Wireshark applies its display filters to discard uninteresting packets, and then decodes and displays the remaining packets.

.pcap File Display

Wireshark can decode and display packets from a previously stored .pcap file and direct the display filter to selectively displayed packets.

Packet Storage and Display

Functionally, this mode is a combination of the previous two modes. Wireshark stores packets in the specified .pcap file and decodes and displays them to the console. Only the core filters are applicable here.

Wireshark Capture Point Activation and Deactivation

After a Wireshark capture point has been defined with its attachment points, filters, actions, and other options, it must be activated. Until the capture point is activated, it does not actually capture packets.

Before a capture point is activated, some functional checks are performed. A capture point cannot be activated if it has neither a core system filter nor attachment points defined. Attempting to activate a capture point that does not meet these requirements generates an error.*

Note *When performing a wireless capture with a CAPWAP tunneling interface, the core system filter is not required and cannot be used.

The display filters are specified as needed.

After Wireshark capture points are activated, they can be deactivated in multiple ways. A capture point that is storing only packets to a .pcap file can be halted manually or configured with time or packet limits, after which the capture point halts automatically.

When a Wireshark capture point is activated, a fixed rate policer is applied automatically in the hardware so that the CPU is not flooded with Wireshark-directed packets. The disadvantage of the rate policer is that you cannot capture contiguous packets beyond the established rate even if more resources are available.

The set packet capture rate is 1000 packets per sec (pps). The 1000 pps limit is applied to the sum of all attachment points. For example, if we have a capture session with 3 attachment points, the rates of all 3 attachment points added together is policed to 1000 pps.

Note Policer is not supported for control-plane packet capture. When activating control-plane capture points, you need to be extra cautious, so that it does not flood the CPU.

Wireshark Features

This section describes how Wireshark features function in the switch environment:

- If port security and Wireshark are applied on an ingress capture, a packet that is dropped by port security will still be captured by Wireshark. If port security is applied on an ingress capture, and Wireshark is applied on an egress capture, a packet that is dropped by port security will not be captured by Wireshark.
- Packets dropped by Dynamic ARP Inspection (DAI) are not captured by Wireshark.
- If a port that is in STP blocked state is used as an attachment point and the core filter is matched, Wireshark will capture the packets that come into the port, even though the packets will be dropped by the switch.
- Classification-based security features—Packets that are dropped by input classification-based security features (such as ACLs and IPSG) are not caught by Wireshark capture points that are connected to attachment points at the same layer. In contrast, packets that are dropped by output classification-based security features are caught by Wireshark capture points that are connected to attachment points at the same layer. The logical model is that the Wireshark attachment point occurs after the security feature lookup on the input side, and symmetrically before the security feature lookup on the output side.

On ingress, a packet goes through a Layer 2 port, a VLAN, and a Layer 3 port/SVI. On egress, the packet goes through a Layer 3 port/SVI, a VLAN, and a Layer 2 port. If the attachment point is before the point where the packet is dropped, Wireshark will capture the packet. Otherwise, Wireshark will not capture the packet. For example, Wireshark capture policies connected to Layer 2 attachment points in the input direction capture packets dropped by Layer 3 classification-based security features. Symmetrically, Wireshark capture policies attached to Layer 3 attachment points in the output direction capture packets dropped by Layer 2 classification-based security features.

- Routed ports and switch virtual interfaces (SVIs)—Wireshark cannot capture the output of an SVI because the packets that go out of an SVI's output are generated by CPU. To capture these packets, include the control plane as an attachment point.
- VLANs—Starting with Cisco IOS Release 16.1, when a VLAN is used as a Wireshark attachment point, packet capture is supported on L2 and L3 in both input and output directions.
- Redirection features—In the input direction, features traffic redirected by Layer 3 (such as PBR and WCCP) are logically later than Layer 3 Wireshark attachment points. Wireshark captures these packets even though they might later be redirected out another Layer 3 interface. Symmetrically, output features redirected by Layer 3 (such as egress WCCP) are logically prior to Layer 3 Wireshark attachment points, and Wireshark will not capture them.
- SPAN—Wireshark cannot capture packets on interface configured as a SPAN destination.
- SPAN—Wireshark is able to capture packets on interfaces configured as a SPAN source in the ingress direction, and may be available for egress direction too.
- You can capture packets from a maximum of 1000 VLANs at a time, if no ACLs are applied. If ACLs are applied, the hardware will have less space for Wireshark to use. As a result, the maximum number of VLANs than can be used for packet capture at a time will be lower. Using more than 1000 VLANs tunnels at a time or extensive ACLs might have unpredictable results. For example, mobility may go down.

Note Capturing an excessive number of attachment points at the same time is strongly discouraged because it may cause excessive CPU utilization and unpredictable hardware behavior.

Wireless Packet Capture in Wireshark

- Wireless traffic is encapsulated inside CAPWAP packets. However, capturing only a particular wireless client's traffic inside a CAPWAP tunnel is not supported when using the CAPWAP tunnel as an attachment point. To capture only a particular wireless client's traffic, use the client VLAN as an attachment point and formulate the core filter accordingly.
- Limited decoding of inner wireless traffic is supported. Decoding of inner wireless packets inside encrypted CAPWAP tunnels is not supported.
- No other interface type can be used with the CAPWAP tunneling interface on the same capture point. A CAPWAP tunneling interface and a Level 2 port cannot be attachment points on the same capture point.
- You cannot specify a core filter when capturing packets for Wireshark via the CAPWAP tunnel. However, you can use the Wireshark display filters for filtering wireless client traffic against a specific wireless client.

- You can capture packets from a maximum of 135 CAPWAP tunnels at a time if no ACLs are applied. If ACLs are applied, the hardware memory will have less space for Wireshark to use. As a result, the maximum number of CAPWAP tunnels than can be used for packet capture at a time will be lower. Using more than 135 CAPWAP tunnels at a time or unsing extensive ACLs might have unpredictable results. For example, mobility may go down.

Note Capturing an excessive number of attachment points at the same time is strongly discouraged because it may cause excessive CPU utilization and unpredictable hardware behavior.

Guidelines for Wireshark

- During Wireshark packet capture, hardware forwarding happens concurrently.
- Before starting a Wireshark capture process, ensure that CPU usage is moderate and that sufficient memory (at least 200 MB) is available.
- If you plan to store packets to a storage file, ensure that sufficient space is available before beginning a Wireshark capture process.
- The CPU usage during Wireshark capture depends on how many packets match the specified conditions and on the intended actions for the matched packets (store, decode and display, or both).
- Where possible, keep the capture to the minimum (limit by packets, duration) to avoid high CPU usage and other undesirable conditions.
- Because packet forwarding typically occurs in hardware, packets are not copied to the CPU for software processing. For Wireshark packet capture, packets are copied and delivered to the CPU, which causes an increase in CPU usage.

  To avoid high CPU usage, do the following:

  - Attach only relevant ports.
  - Use a class map, and secondarily, an access list to express match conditions. If neither is viable, use an explicit, in-line filter.
  - Adhere closely to the filter rules. Restrict the traffic type (such as, IPv4 only) with a restrictive, rather than relaxed ACL, which elicits unwanted traffic.

- Always limit packet capture to either a shorter duration or a smaller packet number. The parameters of the capture command enable you to specify the following:

  - Capture duration
  - Number of packets captured
  - File size
  - Packet segment size

- Run a capture session without limits if you know that very little traffic matches the core filter.

- You might experience high CPU (or memory) usage if:
  - You leave a capture session enabled and unattended for a long period of time, resulting in unanticipated bursts of traffic.
  - You launch a capture session with ring files or capture buffer and leave it unattended for a long time, resulting in performance or system health issues.
- During a capture session, watch for high CPU usage and memory consumption due to Wireshark that may impact switch performance or health. If these situations arise, stop the Wireshark session immediately.
- Avoid decoding and displaying packets from a .pcap file for a large file. Instead, transfer the .pcap file to a PC and run Wireshark on the PC.
- You can define up to eight Wireshark instances. An active **show** command that decodes and displays packets from a .pcap file or capture buffer counts as one instance. However, only one of the instances can be active.
- Whenever an ACL that is associated with a running capture is modified, you must restart the capture for the ACL modifications to take effect. If you do not restart the capture, it will continue to use the original ACL as if it had not been modified.
- To avoid packet loss, consider the following:
  - Use store-only (when you do not specify the display option) while capturing live packets rather than decode and display, which is an CPU-intensive operation (especially in detailed mode).
  - If you have more than one capture that is storing packets in a buffer, clear the buffer before starting a new capture to avoid memory loss.
  - If you use the default buffer size and see that you are losing packets, you can increase the buffer size to avoid losing packets.
  - Writing to flash disk is a CPU-intensive operation, so if the capture rate is insufficient, you may want to use a buffer capture.
  - The Wireshark capture session always operates in streaming mode at the rate of 1000 pps.
- The streaming capture mode rate is 1000 pps.
- If you want to decode and display live packets in the console window, ensure that the Wireshark session is bounded by a short capture duration.

Warning A Wireshark session with either a longer duration limit or no capture duration (using a terminal with no auto-more support using the **term len 0** command) may make the console or terminal unusable.

- When using Wireshark to capture live traffic that leads to high CPU, usage, consider applying a QoS policy temporarily to limit the actual traffic until the capture process concludes.
- All Wireshark-related commands are in EXEC mode; no configuration commands exist for Wireshark.

  If you need to use access list or class-map in the Wireshark CLI, you must define an access list and class map with configuration commands.

- No specific order applies when defining a capture point; you can define capture point parameters in any order, provided that CLI allows this. The Wireshark CLI allows as many parameters as possible on a single line. This limits the number of commands required to define a capture point.
- All parameters except attachment points take a single value. Generally, you can replace the value with a new one by reentering the command. After user confirmation, the system accepts the new value and overrides the older one. A **no** form of the command is unnecessary to provide a new value, but it is necessary to remove a parameter.
- Wireshark allows you to specify one or more attachment points. To add more than one attachment point, reenter the command with the new attachment point. To remove an attachment point, use the **no** form of the command. You can specify an interface range as an attachment point. For example, enter **monitor capture mycap interface GigabitEthernet1/0/1 in** where interface GigabitEthernet1/0/1 is an attachment point.

  If you also need to attach interface GigabitEthernet1/0/2, specify it in another line as follows:

  monitor capture mycap interface GigabitEthernet1/0/2 in
- You cannot make changes to a capture point when the capture is active.
- The action you want to perform determines which parameters are mandatory. The Wireshark CLI allows you to specify or modify any parameter prior to entering the **start** command. When you enter the **start** command, Wireshark will start only after determining that all mandatory parameters have been provided.
- If the file already exists at the time of creation of the capture point, Wireshark queries you as to whether the file can be overwritten. If the file already exists at the time of activating the capture point, Wireshark will overwrite the existing file.
- The core filter can be an explicit filter, access list, or class map. Specifying a newer filter of these types replaces the existing one.

Note A core filter is required except when using a CAPWAP tunnel interface as a capture point attachment point.

- You can terminate a Wireshark session with an explicit **stop** command or by entering **q** in automore mode. The session could terminate itself automatically when a stop condition such as duration or packet capture limit is met, or if an internal error occurs, or resource is full (specifically if disk is full in file mode).
- Dropped packets will not be shown at the end of the capture. However, only the count of dropped, oversized packets will be displayed.

Default Wireshark Configuration

The table below shows the default Wireshark configuration.

Feature	Default Setting
Duration	No limit
Packets	No limit

Feature	Default Setting
Packet-length	No limit (full packet)
File size	No limit
Ring file storage	No
Buffer storage mode	Linear

How to Configure Wireshark

To configure Wireshark, perform these basic steps.

1. Define a capture point.
2. (Optional) Add or modify the capture point's parameters.
3. Activate or deactivate a capture point.
4. Delete the capture point when you are no longer using it.

Related Topics

Defining a Capture Point, on page 553
Adding or Modifying Capture Point Parameters, on page 558
Deleting Capture Point Parameters, on page 560
Deleting a Capture Point, on page 562
Activating and Deactivating a Capture Point, on page 563
Clearing the Capture Point Buffer, on page 566
Example: Simple Capture and Display, on page 571
Example: Simple Capture and Store, on page 572
Example: Using Buffer Capture, on page 575
Example: Capture Sessions, on page 581
Example: Capture and Store in Lock-step Mode, on page 582
Example: Simple Capture and Store of Packets in Egress Direction, on page 583

Defining a Capture Point

The example in this procedure defines a very simple capture point. If you choose, you can define a capture point and all of its parameters with one instance of the **monitor capture** command.

Note You must define an attachment point, direction of capture, and core filter to have a functional capture point.

An exception to needing to define a core filter is when you are defining a wireless capture point using a CAPWAP tunneling interface. In this case, you do not define your core filter. It cannot be used.

Follow these steps to define a capture point.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show capwap summary** **Example:** `Switch# show capwap summary`	Displays the CAPWAP tunnels available as attachment points for a wireless capture. **Note** Use this command only if you are using a CAPWAP tunnel as an attachment point to perform a wireless capture. See the CAPWAP example in the examples section.
Step 3	**monitor capture** {*capture-name*} {**interface** *interface-type interface-id* | **control-plane**} {**in** | **out** | **both**} **Example:** `Switch# monitor capture mycap interface GigabitEthernet1/0/1 in`	Defines the capture point, specifies the attachment point with which the capture point is associated, and specifies the direction of the capture. The keywords have these meanings: • *capture-name*—Specifies the name of the capture point to be defined (mycap is used in the example). Capture Name should be less than or equal to 8 characters. Only alphanumeric characters and underscore (_) is permitted • (Optional) **interface** *interface-type interface-id*—Specifies the attachment point with which the capture point is associated (GigabitEthernet1/0/1 is used in the example). **Note** Optionally, you can define multiple attachment points and all of the parameters for this capture point with this one command instance. These parameters are discussed in the instructions for modifying capture point parameters. Range support is also available both for adding and removing attachment points. Use one of the following for *interface-type*:

	Command or Action	Purpose
		• **GigabitEthernet**—Specifies the attachment point as GigabitEthernet. • **vlan**—Specifies the attachment point as a VLAN. **Note** Only ingress capture (in) is allowed when using this interface as an attachment point. • **capwap**—Specifies the attachment point as a CAPWAP tunnel. **Note** When using this interface as an attachment point, a core filter cannot be used. • (Optional) **control-plane**—Specifies the control plane as an attachment point. • **in** | **out** | **both**—Specifies the direction of capture.
Step 4	**monitor capture** {*capture-name*} [**match** {**any** | **ipv4 any any** | **ipv6**} **any any**}] **Example:** `Switch# monitor capture mycap interface GigabitEthernet1/0/1 in match any`	Defines the core system filter. **Note** When using the CAPWAP tunneling interface as an attachment point, do not perform this step because a core filter cannot be used. The keywords have these meanings: • *capture-name*—Specifies the name of the capture point to be defined (mycap is used in the example). • **match**—Specifies a filter. The first filter defined is the core filter. **Note** A capture point cannot be activated if it has neither a core system filter nor attachment points defined. Attempting to activate a capture point that does not meet these requirements generates an error. • **ipv4**—Specifies an IP version 4 filter. • **ipv6**—Specifies an IP version 6 filter.

	Command or Action	Purpose

Step 5	**show monitor capture** {*capture-name*}[**parameter**]
	Example:
	`Switch# show monitor capture mycap parameter`
	`monitor capture mycap interface GigabitEthernet1/0/1 in`
	`monitor capture mycap match any`
		Displays the capture point parameters that you defined in Step 2 and confirms that you defined a capture point.

Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Example

To define a capture point with a CAPWAP attachment point:

```
Switch# show capwap summary

CAPWAP Tunnels General Statistics:
  Number of Capwap Data Tunnels       = 1
  Number of Capwap Mobility Tunnels   = 0
  Number of Capwap Multicast Tunnels  = 0


Name   APName                           Type PhyPortIf Mode      McastIf
------ -------------------------------- ---- --------- --------- -------
Ca0    AP442b.03a9.6715                 data Gi3/0/6   unicast   -


Name   SrcIP           SrcPort DestIP          DstPort DtlsEn MTU   Xact
------ --------------- ------- --------------- ------- ------ ----- ----
Ca0    10.10.14.32     5247    10.10.14.2      38514   No     1449  0

Switch# monitor capture mycap interface capwap 0 both
Switch# monitor capture mycap file location flash:mycap.pcap
Switch# monitor capture mycap file buffer-size 1
Switch# monitor capture mycap start

*Aug 20 11:02:21.983: %BUFCAP-6-ENABLE: Capture Point mycap enabled.on

Switch# show monitor capture mycap parameter
   monitor capture mycap interface capwap  0 in
   monitor capture mycap interface capwap  0 out
   monitor capture mycap file location flash:mycap.pcap buffer-size 1
Switch#
```

```
Switch# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
  Interface: CAPWAP,
    Ingress:
 0
    Egress:
 0
   Status : Active
  Filter Details:
    Capture all packets
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
   Size of buffer(in MB): 1
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
Switch#
Switch# show monitor capture file flash:mycap.pcap
  1   0.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  2   0.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  3   2.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  4   2.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  5   3.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  6   4.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  7   4.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  8   5.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  9   5.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 10   6.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 11   8.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 12   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 13   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 14   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 15   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 16   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 17   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 18   9.236987   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 19  10.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 20  10.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 21  12.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 22  12.239993   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 23  12.244997   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 24  12.244997   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 25  12.250994   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
```

```
26  12.256990   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
27  12.262987   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
28  12.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=........
29  12.802012   10.10.14.3 -> 10.10.14.255 NBNS Name query NB WPAD.<00>
30  13.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=........
```

What to do next

You can add additional attachment points, modify the parameters of your capture point, then activate it, or if you want to use your capture point just as it is, you can now activate it.

Note You cannot change a capture point's parameters using the methods presented in this topic.

If the user enters an incorrect capture name, or an invalid/non existing attachment point, the switch will show errors like "*Capture Name should be less than or equal to 8 characters. Only alphanumeric characters and underscore (_) is permitted*" and "*% Invalid input detected at '^' marker*" respectively.

Related Topics

How to Configure Wireshark, on page 553
Capture Points, on page 543
Attachment Points, on page 544
Example: Simple Capture and Display, on page 571
Example: Simple Capture and Store, on page 572
Example: Using Buffer Capture, on page 575
Example: Capture Sessions, on page 581
Example: Capture and Store in Lock-step Mode, on page 582
Example: Simple Capture and Store of Packets in Egress Direction, on page 583

Adding or Modifying Capture Point Parameters

Although listed in sequence, the steps to specify values for the parameters can be executed in any order. You can also specify them in one, two, or several lines. Except for attachment points, which can be multiple, you can replace any value with a more recent value by redefining the same option. You will need to confirm interactively when certain parameters already specified are being modified.

Follow these steps to modify a capture point's parameters.

Before you begin

A capture point must be defined before you can use these instructions.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Switch> enable`	
Step 2	**monitor capture** {*capture-name*} **match** {**any** | **mac** *mac-match-string* | **ipv4** {**any** | **host** | **protocol**}{**any** | **host**} | **ipv6** {**any** | **host** | **protocol**}{**any** | **host**}} **Example:** `Switch# monitor capture mycap match ipv4 any any`	Defines the core system filter (**ipv4 any any**), defined either explicitly, through ACL or through a class map. **Note** If you are defining a wireless capture point using a CAPWAP tunneling interface, this command will have no effect, so it should not be used.
Step 3	**monitor capture** {*capture-name*} **limit** {[**duration** *seconds*][**packet-length** *size*][**packets** *num*]} **Example:** `Switch# monitor capture mycap limit duration 60 packet-len 400`	Specifies the session limit in seconds (60), packets captured, or the packet segment length to be retained by Wireshark (400).
Step 4	**monitor capture** {*capture-name*} **file** {**location** *filename*} **Example:** `Switch# monitor capture mycap file location flash:mycap.pcap`	Specifies the file association, if the capture point intends to capture packets rather than only display them. **Note** If the file already exists, you have to confirm if it can be overwritten. **Note** File option does not exist on LAN base license.
Step 5	**monitor capture** {*capture-name*} **file** {**buffer-size** *size*} **Example:** `Switch# monitor capture mycap file buffer-size 100`	Specifies the size of the memory buffer used by Wireshark to handle traffic bursts.

Step 6	**show monitor capture** {*capture-name*}[**parameter**]
	Example:
	`Switch# show monitor capture mycap parameter`
	`monitor capture mycap interface GigabitEthernet1/0/1 in`
	`monitor capture mycap match ipv4 any any`
	`monitor capture mycap limit duration 60 packet-len 400`
	`monitor capture point mycap file location bootdisk:mycap.pcap`
	`monitor capture mycap file buffer-size 100`
		Displays the capture point parameters that you defined previously.

	Command or Action	Purpose
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Examples

Modifying Parameters

Associating or Disassociating a Capture File

```
Switch# monitor capture point mycap file location flash:mycap.pcap
Switch# no monitor capture mycap file
```

Specifying a Memory Buffer Size for Packet Burst Handling

```
Switch# monitor capture mycap buffer size 100
```

Defining an Explicit Core System Filter to Match Both IPv4 and IPv6

```
Switch# monitor capture mycap match any
```

What to do next

if your capture point contains all of the parameters you want, activate it.

Related Topics

How to Configure Wireshark, on page 553
Capture Points, on page 543
Attachment Points, on page 544
Example: Simple Capture and Display, on page 571
Example: Simple Capture and Store, on page 572
Example: Using Buffer Capture, on page 575
Example: Capture Sessions, on page 581
Example: Capture and Store in Lock-step Mode, on page 582
Example: Simple Capture and Store of Packets in Egress Direction, on page 583

Deleting Capture Point Parameters

Although listed in sequence, the steps to delete parameters can be executed in any order. You can also delete them in one, two, or several lines. Except for attachment points, which can be multiple, you can delete any parameter.

Follow these steps to delete a capture point's parameters.

Before you begin

A capture point parameter must be defined before you can use these instructions to delete it.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**no monitor capture** {*capture-name*} **match** **Example:** `Switch# no monitor capture mycap match`	Deletes all filters defined on capture point (mycap).

Step 3	**no monitor capture** {*capture-name*} **limit** [**duration**] [**packet-length**] [**packets**]
	Example:
	`Switch# no monitor capture mycap limit duration packet-len`
	`Switch# no monitor capture mycap limit`
		Deletes the session time limit and the packet segment length to be retained by Wireshark. It leaves other specified limits in place.
		Deletes all limits on Wireshark.

Step 4	**no monitor capture** {*capture-name*} **file** [**location**] [**buffer-size**]
	Example:
	`Switch# no monitor capture mycap file`
	`Switch# no monitor capture mycap file location`
		Deletes the file association. The capture point will no longer capture packets. It will only display them.
		Deletes the file location association. The file location will no longer be associated with the capture point. However, other defined fille association will be unaffected by this action.

Step 5	**show monitor capture** {*capture-name*}[**parameter**]
	Example:
	`Switch# show monitor capture mycap parameter`
	`monitor capture mycap interface GigabitEthernet1/0/1 in`
		Displays the capture point parameters that remain defined after your parameter deletion operations. This command can be run at any point in the procedure to see what parameters are associated with a capture point.

Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

What to do next

If your capture point contains all of the parameters you want, activate it.

Note If the parameters are deleted when the capture point is active, the switch will show an error "*Capture is active*".

Related Topics

How to Configure Wireshark, on page 553
Capture Points, on page 543
Attachment Points, on page 544
Example: Simple Capture and Display, on page 571
Example: Simple Capture and Store, on page 572
Example: Using Buffer Capture, on page 575
Example: Capture Sessions, on page 581
Example: Capture and Store in Lock-step Mode, on page 582
Example: Simple Capture and Store of Packets in Egress Direction, on page 583

Deleting a Capture Point

Follow these steps to delete a capture point.

Before you begin

A capture point must be defined before you can use these instructions to delete it. You have to stop the capture point before you can delete it.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**no monitor capture** {*capture-name*} **Example:** `Switch# no monitor capture mycap`	Deletes the specified capture point (mycap).

Step 3	**show monitor capture** {*capture-name*} [**parameter**]
	Example:
	`Switch# show monitor capture mycap parameter`
	`Capture mycap does not exist`
		Displays a message indicating that the specified capture point does not exist because it has been deleted.

Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:**	Verifies your entries.

	Command or Action	Purpose
	`Switch# show running-config`	
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

You can define a new capture point with the same name as the one you deleted. These instructions are usually performed when one wants to start over with defining a capture point.

Related Topics

How to Configure Wireshark, on page 553
Capture Points, on page 543
Attachment Points, on page 544
Example: Simple Capture and Display, on page 571
Example: Simple Capture and Store, on page 572
Example: Using Buffer Capture, on page 575
Example: Capture Sessions, on page 581
Example: Capture and Store in Lock-step Mode, on page 582
Example: Simple Capture and Store of Packets in Egress Direction, on page 583

Activating and Deactivating a Capture Point

Follow these steps to activate or deactivate a capture point.

Before you begin

A capture point can be activated even if an attachment point and a core system filter have been defined and the associated filename already exists. In such an instance, the existing file will be overwritten.

A capture point with no associated filename can only be activated to display. When the filename is not specified, the packets are captured into the buffer. Live display (display during capture) is available in both file and buffer modes.

If no display filters are specified, packets are not displayed live, and all the packets captured by the core system filter are displayed. The default display mode is brief.

Note When using a CAPWAP tunneling interface as an attachment point, core filters are not used, so there is no requirement to define them in this case.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**monitor capture** {*capture-name*} **start** [**display** [**display-filter** *filter-string*]] [**brief** | **detailed** | **dump**] **Example:** `Switch# monitor capture mycap start display display-filter "stp"`	Activates a capture point and filters the display, so only packets containing "stp" are displayed.
Step 3	**monitor capture** {*capture-name*} **stop** **Example:** `Switch# monitor capture name stop`	Deactivates a capture point.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

While activating and deactivating a capture point, you could encounter a few errors. Here are examples of some of the possible errors.

Missing attachment point on activation

```
Switch#monitor capture mycap match any
Switch#monitor capture mycap start
No Target is attached to capture failed to disable provision featurefailed to remove
policyfailed to disable provision featurefailed to remove policyfailed to disable provision
 featurefailed to remove policy
Capture statistics collected at software (Buffer):
```

```
 Capture duration - 0 seconds
 Packets received - 0
 Packets dropped - 0
 Packets oversized - 0

Unable to activate Capture.
Switch# unable to get action unable to get action unable to get action
Switch#monitor capture mycap interface g1/0/1 both
Switch#monitor capture mycap start
Switch#
*Nov 5 12:33:43.906: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
```

Missing filter on activation

```
Switch#monitor capture mycap int g1/0/1 both
Switch#monitor capture mycap start
Filter not attached to capture
Capture statistics collected at software (Buffer):
 Capture duration - 0 seconds
 Packets received - 0
 Packets dropped - 0
 Packets oversized - 0

Unable to activate Capture.
Switch#monitor capture mycap match any
Switch#monitor capture mycap start
Switch#
*Nov 5 12:35:37.200: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
```

Attempting to activate a capture point while another one is already active

```
Switch#monitor capture mycap start
PD start invoked while previous run is active Failed to start capture : Wireshark operation
 failure
Unable to activate Capture.
Switch#show monitor capture

Status Information for Capture test
 Target Type:
 Interface: GigabitEthernet1/0/13, Direction: both
 Interface: GigabitEthernet1/0/14, Direction: both
 Status : Active
 Filter Details:
 Capture all packets
 Buffer Details:
 Buffer Type: LINEAR (default)
 Buffer Size (in MB): 10
 File Details:
 Associated file name: flash:cchh.pcap
 Limit Details:
 Number of Packets to capture: 0 (no limit)
 Packet Capture duration: 0 (no limit)
 Packet Size to capture: 0 (no limit)
 Maximum number of packets to capture per second: 1000
 Packet sampling rate: 0 (no sampling)

Status Information for Capture mycap
 Target Type:
 Interface: GigabitEthernet1/0/1, Direction: both
 Status : Inactive
 Filter Details:
 Capture all packets
 Buffer Details:
 Buffer Type: LINEAR (default)
 Buffer Size (in MB): 10
```

```
 File Details:
 File not associated
 Limit Details:
 Number of Packets to capture: 0 (no limit)
 Packet Capture duration: 0 (no limit)
 Packet Size to capture: 0 (no limit)
 Maximum number of packets to capture per second: 1000
 Packet sampling rate: 0 (no sampling)
Switch#monitor capture test stop
Capture statistics collected at software (Buffer & Wireshark):
 Capture duration - 157 seconds
 Packets received - 0
 Packets dropped - 0
 Packets oversized - 0

Switch#
*Nov 5 13:18:17.406: %BUFCAP-6-DISABLE: Capture Point test disabled.
Switch#monitor capture mycap start
Switch#
*Nov 5 13:18:22.664: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
Switch#
```

Related Topics

How to Configure Wireshark, on page 553
Capture Points, on page 543
Attachment Points, on page 544
Example: Simple Capture and Display, on page 571
Example: Simple Capture and Store, on page 572
Example: Using Buffer Capture, on page 575
Example: Capture Sessions, on page 581
Example: Capture and Store in Lock-step Mode, on page 582
Example: Simple Capture and Store of Packets in Egress Direction, on page 583

Clearing the Capture Point Buffer

Follow these steps to clear the buffer contents or save them to an external file for storage.

Note If you have more than one capture that is storing packets in a buffer, clear the buffer before starting a new capture to avoid memory loss. Do not try to clear buffer on an active capture point.

Note Clearing buffer on an active capture point is supported only on Lan Base as this only clears the content. On all other licenses, it deletes the buffer itself, hence cannot be run during active capture.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Switch> enable`	
Step 2	**monitor capture** {*capture-name*} [**clear** | **export** *filename*] **Example:** `Switch# monitor capture mycap clear`	Clear - Completely deletes the buffer. **Note** When the clear command is run, • On Lan base - the command clears the buffer contents without deleting the buffer • On all other licenses - the command deletes the buffer itself. Export - Saves the captured packets in the buffer as well as deletes the buffer.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 4	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 5	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Examples: Capture Point Buffer Handling

Exporting Capture to a File

```
Switch# monitor capture mycap export flash:mycap.pcap

Storage configured as File for this capture
```

Clearing Capture Point Buffer

```
Switch# monitor capture mycap clear

 Capture configured with file options
```

What to do next

Note If you try to clear the capture point buffer on licenses other than LAN Base, the switch will show an error "*Failed to clear capture buffer : Capture Buffer BUSY*".

Related Topics

How to Configure Wireshark, on page 553
Capture Points, on page 543
Attachment Points, on page 544
Example: Simple Capture and Display, on page 571
Example: Simple Capture and Store, on page 572
Example: Using Buffer Capture, on page 575
Example: Capture Sessions, on page 581
Example: Capture and Store in Lock-step Mode, on page 582
Example: Simple Capture and Store of Packets in Egress Direction, on page 583

Monitoring Wireshark

The commands in this table are used to monitor Wireshark.

Command	Purpose
show monitor capture [*capture-name*]	Displays the capture point state so that you can see what capture points are defined, what their attributes are, and whether they are active. When capture point name is specified, it displays specific capture point's details.
show monitor capture [*capture-name* **parameter**]	Displays the capture point parameters.
show capwap summary	Displays all the CAPWAP tunnels on the switch. Use this command to determine which CAPWAP tunnels are available to use for a wireless capture.

Configuration Examples for Wireshark

Example: Displaying a Brief Output from a .pcap File

You can display the output from a .pcap file by entering:

```
Switch# show monitor capture file flash:mycap.pcap brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit
```

```
  1 0.000000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=0/0, ttl=254
  2 0.000051000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=0/0, ttl=255 (request in 1)
  3 0.000908000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=1/256, ttl=254
  4 0.001782000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=1/256, ttl=255 (request in 3)
  5 0.002961000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=2/512, ttl=254
  6 0.003676000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=2/512, ttl=255 (request in 5)
  7 0.004835000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=3/768, ttl=254
  8 0.005579000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=3/768, ttl=255 (request in 7)
  9 0.006850000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=4/1024, ttl=254
 10 0.007586000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=4/1024, ttl=255 (request in 9)
 11 0.008768000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=5/1280, ttl=254
 12 0.009497000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=5/1280, ttl=255 (request in 11)
 13 0.010695000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=6/1536, ttl=254
 14 0.011427000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=6/1536, ttl=255 (request in 13)
 15 0.012728000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=7/1792, ttl=254
 16 0.013458000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=7/1792, ttl=255 (request in 15)
 17 0.014652000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=8/2048, ttl=254
 18 0.015394000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=8/2048, ttl=255 (request in 17)
 19 0.016682000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=9/2304, ttl=254
 20 0.017439000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=9/2304, ttl=255 (request in 19)
 21 0.018655000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=10/2560, ttl=254
 22 0.019385000   10.10.10.1 -> 10.10.10.2   ICMP 114 Echo (ping) reply    id=0x002e,
seq=10/2560, ttl=255 (request in 21)
 23 0.020575000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x002e,
seq=11/2816, ttl=254
 --More‹
```

Example: Displaying Detailed Output from a .pcap File

You can display the detailed .pcap file output by entering:

```
Switch# show monitor capture file flash:mycap.pcap detailed
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

Frame 1: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
    Interface id: 0
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov  6, 2015 11:44:48.322497000 UTC
    [Time shift for this packet: 0.000000000 seconds]
```

```
    Epoch Time: 1446810288.322497000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 114 bytes (912 bits)
    Capture Length: 114 bytes (912 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:icmp:data]
Ethernet II, Src: Cisco_f3:63:46 (00:e1:6d:f3:63:46), Dst: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)

    Destination: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)
        Address: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Cisco_f3:63:46 (00:e1:6d:f3:63:46)
        Address: Cisco_f3:63:46 (00:e1:6d:f3:63:46)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
Internet Protocol Version 4, Src: 10.10.10.2 (10.10.10.2), Dst: 10.10.10.1 (10.10.10.1)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not
ECN-Capable Transport))
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport)
(0x00)
    Total Length: 100
    Identification: 0x04ba (1210)
    Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 254
    Protocol: ICMP (1)
    Header checksum: 0x8fc8 [validation disabled]
        [Good: False]
        [Bad: False]
    Source: 10.10.10.2 (10.10.10.2)
    Destination: 10.10.10.1 (10.10.10.1)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xe4db [correct]
    Identifier (BE): 46 (0x002e)
    Identifier (LE): 11776 (0x2e00)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    Data (72 bytes)

0000  00 00 00 00 09 c9 8f 77 ab cd ab cd ab cd ab cd   .......w........
0010  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0020  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0030  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0040  ab cd ab cd ab cd ab cd                           ........
        Data: 0000000009c98f77abcdabcdabcdabcdabcdabcdabcdabcd...
        [Length: 72]

Frame 2: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
    Interface id: 0
```

Example: Simple Capture and Display

This example shows how to monitor traffic in the Layer 3 interface Gigabit Ethernet 1/0/1:

Step 1: Define a capture point to match on the relevant traffic by entering:

```
Switch# monitor capture mycap interface GigabitEthernet1/0/3 in
Switch# monitor capture mycap match ipv4 any any
Switch# monitor capture mycap limit duration 60 packets 50
Switch# monitor capture mycap buffer size 100
```

To avoid high CPU utilization, a low packet count and duration as limits has been set.

Step 2: Confirm that the capture point has been correctly defined by entering:

```
Switch# show monitor capture mycap parameter
      monitor capture mycap interface GigabitEthernet1/0/3 in
   monitor capture mycap match ipv4  any any
   monitor capture mycap buffer size 100
   monitor capture mycap limit packets 50 duration 60

Switch# show monitor capture mycap
Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/3, Direction: in
   Status : Inactive
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: LINEAR (default)
   Buffer Size (in MB): 100
  File Details:
   File not associated
  Limit Details:
   Number of Packets to capture: 50
   Packet Capture duration: 60
   Packet Size to capture: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
```

Step 3: Start the capture process and display the results.

```
Switch# monitor capture mycap start display
 Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1   0.000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030, seq=0/0,
 ttl=254
  2   0.003682   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=1/256, ttl=254
  3   0.006586   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=2/512, ttl=254
  4   0.008941   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=3/768, ttl=254
  5   0.011138   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=4/1024, ttl=254
  6   0.014099   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=5/1280, ttl=254
  7   0.016868   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=6/1536, ttl=254
  8   0.019210   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
```

```
seq=7/1792, ttl=254
  9   0.024785   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0030,
seq=8/2048, ttl=254
 --More--
```

Step 4: Delete the capture point by entering:

```
Switch# no monitor capture mycap
```

Note A **stop** command is not required in this particular case since we have set a limit and the capture will automatically stop once that limit is reached.

For more information on syntax to be used for pcap statistics, refer the "*Additional References*" section.

Related Topics

Defining a Capture Point, on page 553
Adding or Modifying Capture Point Parameters, on page 558
Deleting Capture Point Parameters, on page 560
Deleting a Capture Point, on page 562
Activating and Deactivating a Capture Point, on page 563
Clearing the Capture Point Buffer, on page 566
How to Configure Wireshark, on page 553
Capture Points, on page 543
Attachment Points, on page 544

Example: Simple Capture and Store

This example shows how to capture packets to a filter:

Step 1: Define a capture point to match on the relevant traffic and associate it to a file by entering:

```
Switch# monitor capture mycap interface GigabitEthernet1/0/3 in
Switch# monitor capture mycap match ipv4 any any
Switch# monitor capture mycap limit duration 60 packets 50
Switch# monitor capture mycap file location flash:mycap.pcap
```

Step 2: Confirm that the capture point has been correctly defined by entering:

```
Switch# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/3 in
   monitor capture mycap match ipv4  any any
   monitor capture mycap file location flash:mycap.pcap
   monitor capture mycap limit packets 50 duration 60

Switch# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/3, Direction: in
   Status : Inactive
  Filter Details:
```

```
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
  Limit Details:
   Number of Packets to capture: 50
   Packet Capture duration: 60
   Packet Size to capture: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
```

Step 3: Launch packet capture by entering:

```
Switch# monitor capture mycap start
```

Step 4: Display extended capture statistics during runtime by entering:

```
Switch#  show monitor capture mycap capture-statistics
Capture statistics collected at software:
        Capture duration - 15 seconds
        Packets received - 40
        Packets dropped - 0
        Packets oversized - 0
        Packets errored - 0
        Packets sent - 40
        Bytes received - 7280
        Bytes dropped - 0
        Bytes oversized - 0
        Bytes errored - 0
        Bytes sent ¬ 4560
```

Step 5: After sufficient time has passed, stop the capture by entering:

```
Switch# monitor capture mycap stop
Capture statistics collected at software (Buffer & Wireshark):
        Capture duration - 20 seconds
        Packets received - 50
        Packets dropped - 0
        Packets oversized - 0
```

Note Alternatively, you could allow the capture operation stop automatically after the time has elapsed or the packet count has been met.

The mycap.pcap file now contains the captured packets.

Step 6: Display extended capture statistics after stop by entering:

```
Switch#  show monitor capture mycap capture-statistics
Capture statistics collected at software:
        Capture duration - 20 seconds
        Packets received - 50
        Packets dropped - 0
        Packets oversized - 0
        Packets errored - 0
        Packets sent - 50
        Bytes received - 8190
```

```
        Bytes dropped - 0
        Bytes oversized - 0
        Bytes errored - 0
        Bytes sent ¬ 5130
```

Step 7: Display the packets by entering:

```
Switch# show monitor capture file flash:mycap.pcap
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1 0.000000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=0/0, ttl=254
  2 0.002555000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=1/256, ttl=254
  3 0.006199000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=2/512, ttl=254
  4 0.009199000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=3/768, ttl=254
  5 0.011647000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=4/1024, ttl=254
  6 0.014168000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=5/1280, ttl=254
  7 0.016737000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=6/1536, ttl=254
  8 0.019403000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=7/1792, ttl=254
  9 0.022151000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=8/2048, ttl=254
 10 0.024722000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=9/2304, ttl=254
 11 0.026890000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=10/2560, ttl=254
 12 0.028862000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0031,
seq=11/2816, ttl=254
 --More--
```

For more information on syntax to be used for pcap statistics, refer the "*Additional References*" section.

Step 8: Delete the capture point by entering:

```
Switch# no monitor capture mycap
```

Related Topics

Defining a Capture Point, on page 553
Adding or Modifying Capture Point Parameters, on page 558
Deleting Capture Point Parameters, on page 560
Deleting a Capture Point, on page 562
Activating and Deactivating a Capture Point, on page 563
Clearing the Capture Point Buffer, on page 566
How to Configure Wireshark, on page 553
Capture Points, on page 543
Attachment Points, on page 544

Example: Using Buffer Capture

This example shows how to use buffer capture:

Step 1: Launch a capture session with the buffer capture option by entering:

```
Switch# monitor capture mycap interface GigabitEthernet1/0/3 in
Switch# monitor capture mycap match ipv4 any any
Switch# monitor capture mycap buffer circular size 1
Switch# monitor capture mycap start
```

Step 2: Determine whether the capture is active by entering:

```
Switch# show monitor capture mycap
Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/3, Direction: in
   Status : Active
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: CIRCULAR
   Buffer Size (in MB): 1
  File Details:
   File not associated
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)
```

Step 3: Display extended capture statistics during runtime by entering:

```
Switch# show monitor capture mycap capture-statistics
Capture statistics collected at software:
        Capture duration - 88 seconds
        Packets received - 1000
        Packets dropped - 0
        Packets oversized - 0
        Packets errored - 0
        Packets sent - 1000
        Bytes received - 182000
        Bytes dropped - 0
        Bytes oversized - 0
        Bytes errored - 0
        Bytes sent - 114000
```

Step 4: Stop the capture by entering:

```
Switch# monitor capture mycap stop
Capture statistics collected at software (Buffer):
        Capture duration - 2185 seconds
        Packets received - 51500
        Packets dropped - 0
        Packets oversized - 0
```

Step 5: Display extended capture statistics after stop by entering:

```
Switch# show monitor capture mycap capture-statistics
Capture statistics collected at software:
        Capture duration - 156 seconds
        Packets received - 2000
        Packets dropped - 0
        Packets oversized - 0
        Packets errored - 0
        Packets sent - 2000
        Bytes received - 364000
        Bytes dropped - 0
        Bytes oversized - 0
        Bytes errored - 0
        Bytes sent - 228000
```

Step 6: Determine whether the capture is active by entering:

```
Switch# show monitor capture mycap
Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/3, Direction: in
   Status : Inactive
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: CIRCULAR
   Buffer Size (in MB): 1
  File Details:
   File not associated
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)
```

Step 7: Display the packets in the buffer by entering:

```
Switch# show monitor capture mycap buffer brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1   0.000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40057/31132, ttl=254
  2   0.000030   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40058/31388, ttl=254
  3   0.000052   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40059/31644, ttl=254
  4   0.000073   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40060/31900, ttl=254
  5   0.000094   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40061/32156, ttl=254
  6   0.000115   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40062/32412, ttl=254
  7   0.000137   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40063/32668, ttl=254
  8   0.000158   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40064/32924, ttl=254
  9   0.000179   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40065/33180, ttl=254
 10   0.000200   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40066/33436, ttl=254
```

```
 11   0.000221   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40067/33692, ttl=254
 12   0.000243   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0038,
seq=40068/33948, ttl=254
 --More--
```

Notice that the packets have been buffered.

Step 8: Display the packets in other display modes.

```
Switch# show monitor capture mycap buffer detailed
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

Frame 1: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
    Interface id: 0
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov  6, 2015 18:10:06.297972000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1446833406.297972000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 114 bytes (912 bits)
    Capture Length: 114 bytes (912 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:icmp:data]
Ethernet II, Src: Cisco_f3:63:46 (00:e1:6d:f3:63:46), Dst: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)

    Destination: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)
        Address: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Cisco_f3:63:46 (00:e1:6d:f3:63:46)
        Address: Cisco_f3:63:46 (00:e1:6d:f3:63:46)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
Internet Protocol Version 4, Src: 10.10.10.2 (10.10.10.2), Dst: 10.10.10.1 (10.10.10.1)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not
ECN-Capable Transport))
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport)
(0x00)
    Total Length: 100
    Identification: 0xabdd (43997)
    Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 254
    Protocol: ICMP (1)
    Header checksum: 0xe8a4 [validation disabled]
        [Good: False]
        [Bad: False]
    Source: 10.10.10.2 (10.10.10.2)
    Destination: 10.10.10.1 (10.10.10.1)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
```

```
    Checksum: 0xa620 [correct]
    Identifier (BE): 56 (0x0038)
    Identifier (LE): 14336 (0x3800)
    Sequence number (BE): 40057 (0x9c79)
    Sequence number (LE): 31132 (0x799c)
    Data (72 bytes)

0000  00 00 00 00 0b 15 30 63 ab cd ab cd ab cd ab cd   ......0c........
0010  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0020  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0030  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0040  ab cd ab cd ab cd ab cd                           ........
        Data: 000000000b153063abcdabcdabcdabcdabcdabcdabcdabcd...
        [Length: 72]

Frame 2: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0


Switch# show monitor capture mycap buffer dump
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

0000  00 e1 6d 31 f1 c6 00 e1 6d f3 63 46 08 00 45 00   ..m1....m.cF..E.
0010  00 64 ab dd 00 00 fe 01 e8 a4 0a 0a 0a 02 0a 0a   .d..............
0020  0a 01 08 00 a6 20 00 38 9c 79 00 00 00 00 0b 15   ..... .8.y......
0030  30 63 ab cd ab cd ab cd ab cd ab cd ab cd ab cd   0c..............
0040  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0050  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0060  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0070  ab cd                                            ..

0000  00 e1 6d 31 f1 c6 00 e1 6d f3 63 46 08 00 45 00   ..m1....m.cF..E.
0010  00 64 ab de 00 00 fe 01 e8 a3 0a 0a 0a 02 0a 0a   .d..............
0020  0a 01 08 00 a6 1d 00 38 9c 7a 00 00 00 00 0b 15   .......8.z......
0030  30 65 ab cd ab cd ab cd ab cd ab cd ab cd ab cd   0e..............
0040  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0050  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0060  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd   ................
0070  ab cd
```

Step 9: Clear the buffer by entering:

```
Switch# monitor capture mycap clear
```

Note NOTE - Clearing the buffer deletes the buffer along with the contents.

Note If you require the buffer contents to be displayed, run the clear commands after show commands.

Step 10: Restart the traffic, wait for 10 seconds, then display the buffer contents by entering:

Note We cannot run show from buffer during an active capture. Capture should be stopped before running show from buffer. We can however run a show on a pcap file during an active capture in both file and buffer mode. In file mode, we can display the packets in the current capture session's pcap file as well when the capture is active.

```
Switch# monitor capture mycap start
Switch#  show monitor capture mycap

Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/3, Direction: in
   Status : Active
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: CIRCULAR
   Buffer Size (in MB): 1
  File Details:
   File not associated
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)
```

Step 11: Stop the packet capture and display the buffer contents by entering:

```
Switch# monitor capture mycap stop
Capture statistics collected at software (Buffer):
 Capture duration - 111 seconds
 Packets received - 5000
 Packets dropped - 0
 Packets oversized - 0
```

Step 12: Determine whether the capture is active by entering:

```
Switch# show monitor capture mycap
Status Information for Capture mycap
 Target Type:
  Interface: GigabitEthernet1/0/3, Direction: in
 Status : Inactive
Filter Details:
 IPv4
  Source IP: any
  Destination IP: any
 Protocol: any
Buffer Details:
 Buffer Type: CIRCULAR
 Buffer Size (in MB): 1
File Details:
 File not associated
Limit Details:
 Number of Packets to capture: 0 (no limit)
 Packet Capture duration: 0 (no limit)
 Packet Size to capture: 0 (no limit)
```

```
 Maximum number of packets to capture per second: 1000
 Packet sampling rate: 0 (no sampling)
```

Step 13: Display the packets in the buffer by entering:

```
Switch# show monitor capture mycap buffer brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1 0.000000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=0/0, ttl=254
  2 0.000030000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=1/256, ttl=254
  3 0.000051000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=2/512, ttl=254
  4 0.000072000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=3/768, ttl=254
  5 0.000093000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=4/1024, ttl=254
  6 0.000114000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=5/1280, ttl=254
  7 0.000136000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=6/1536, ttl=254
  8 0.000157000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=7/1792, ttl=254
  9 0.000178000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=8/2048, ttl=254
 10 0.000199000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=9/2304, ttl=254
 11 0.000220000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=10/2560, ttl=254
 12 0.000241000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=11/2816, ttl=254
 --More‹
```

Step 14: Store the buffer contents to the mycap.pcap file in the internal flash: storage device by entering:

```
Switch# monitor capture mycap export flash:mycap.pcap
Exported Successfully
```

Note The current implementation of export is such that when the command is run, export is "started" but not complete when it returns the prompt to the user. So we have to wait for a message display on the console from Wireshark before it can run a display of packets in the file.

Step 15: Display capture packets from the file by entering:

```
Switch#  show monitor capture file flash:mycap.pcap
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1 0.000000000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=0/0, ttl=254
  2 0.000030000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=1/256, ttl=254
  3 0.000051000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=2/512, ttl=254
  4 0.000072000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=3/768, ttl=254
  5 0.000093000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=4/1024, ttl=254
```

```
  6 0.000114000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=5/1280, ttl=254
  7 0.000136000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=6/1536, ttl=254
  8 0.000157000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=7/1792, ttl=254
  9 0.000178000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=8/2048, ttl=254
 10 0.000199000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=9/2304, ttl=254
 11 0.000220000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=10/2560, ttl=254
 12 0.000241000   10.10.10.2 -> 10.10.10.1   ICMP 114 Echo (ping) request  id=0x0039,
seq=11/2816, ttl=254
 --More--
```

Step 16: Delete the capture point by entering:

```
Switch# no monitor capture mycap
```

Related Topics

Defining a Capture Point, on page 553
Adding or Modifying Capture Point Parameters, on page 558
Deleting Capture Point Parameters, on page 560
Deleting a Capture Point, on page 562
Activating and Deactivating a Capture Point, on page 563
Clearing the Capture Point Buffer, on page 566
How to Configure Wireshark, on page 553
Capture Points, on page 543
Attachment Points, on page 544

Example: Capture Sessions

```
Switch# monitor capture mycap start display display-filter "stp"
  0.000000 20:37:06:cf:08:b6 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/100/20:37:06:ce:f0:80
  Cost = 0  Port = 0x8136
  2.000992 20:37:06:cf:08:b6 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/100/20:37:06:ce:f0:80
  Cost = 0  Port = 0x8136
  2.981996 20:37:06:cf:08:b6 -> 20:37:06:cf:08:b6 LOOP Reply
  4.000992 20:37:06:cf:08:b6 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/100/20:37:06:ce:f0:80
  Cost = 0  Port = 0x8136
  6.000000 20:37:06:cf:08:b6 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/100/20:37:06:ce:f0:80
  Cost = 0  Port = 0x8136
  7.998001 20:37:06:cf:08:b6 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/100/20:37:06:ce:f0:80
  Cost = 0  Port = 0x8136
  9.998001 20:37:06:cf:08:b6 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/100/20:37:06:ce:f0:80
  Cost = 0  Port = 0x8136
Capture test is not active Failed to Initiate Wireshark
Switch# show monitor capture mycap parameter
   monitor capture mycap control-plane both
   monitor capture mycap match any
   monitor capture mycap file location flash:mycap1.1 buffer-size 90
   monitor capture mycap limit duration 10

Switch# no monitor capture mycap file
Switch# monitor capture mycap start display display-filter "udp.port == 20002" dump
```

```
 Please associate capture file/buffer
Unable to activate Capture.

Switch# monitor capture mycap start display display-filter "udp.port == 20002"
 Please associate capture file/buffer
Unable to activate Capture.

Switch# monitor capture mycap start display detailed
 Please associate capture file/buffer
Unable to activate Capture.
```

Related Topics

Defining a Capture Point, on page 553
Adding or Modifying Capture Point Parameters, on page 558
Deleting Capture Point Parameters, on page 560
Deleting a Capture Point, on page 562
Activating and Deactivating a Capture Point, on page 563
Clearing the Capture Point Buffer, on page 566
How to Configure Wireshark, on page 553
Capture Points, on page 543
Attachment Points, on page 544

Example: Capture and Store in Lock-step Mode

This example captures live traffic and stores the packets in lock-step mode.

Note The capture rate might be slow for the first 15 seconds. If possible and necessary, start the traffic 15 seconds after the capture session starts.

Step 1: Define a capture point to match on the relevant traffic and associate it to a file by entering:

```
Switch# monitor capture mycap interface GigabitEthernet1/0/1 in
Switch# monitor capture mycap match ipv4 any any
Switch# monitor capture mycap limit duration 60 packets 100
Switch# monitor capture mycap file location flash:mycap.pcap buffer-size 64
```

Step 2: Confirm that the capture point has been correctly defined by entering:

```
Switch# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
   monitor capture mycap file location flash:mycap.pcap buffer-size 64
   monitor capture mycap limit packets 100 duration 60

Switch# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/1, Direction: in
   Status : Inactive
  Filter Details:
   Filter not attached
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
```

```
   Size of buffer(in MB): 64
  Limit Details:
   Number of Packets to capture: 100
   Packet Capture duration: 60
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
```

Step 3: Launch packet capture by entering:

```
Switch# monitor capture mycap start
A file by the same capture file name already exists, overwrite?[confirm]
Turning on lock-step mode

Switch#
*Oct 14 09:35:32.661: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
```

Step 4: Display the packets by entering:

```
Switch# show monitor capture file flash:mycap.pcap
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  0.000000    10.1.1.30 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  1.000000    10.1.1.31 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  2.000000    10.1.1.32 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  3.000000    10.1.1.33 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  4.000000    10.1.1.34 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  5.000000    10.1.1.35 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  6.000000    10.1.1.36 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  7.000000    10.1.1.37 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  8.000000    10.1.1.38 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  9.000000    10.1.1.39 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

Step 5: Delete the capture point by entering:

```
Switch# no monitor capture mycap
```

Related Topics

Defining a Capture Point, on page 553
Adding or Modifying Capture Point Parameters, on page 558
Deleting Capture Point Parameters, on page 560
Deleting a Capture Point, on page 562
Activating and Deactivating a Capture Point, on page 563
Clearing the Capture Point Buffer, on page 566
How to Configure Wireshark, on page 553
Capture Points, on page 543
Attachment Points, on page 544

Example: Simple Capture and Store of Packets in Egress Direction

This example shows how to capture packets to a filter:

Step 1: Define a capture point to match on the relevant traffic and associate it to a file by entering:

```
Switch# monitor capture mycap interface Gigabit 1/0/1 out match ipv4 any any
Switch# monitor capture mycap limit duration 60 packets 100
Switch# monitor capture mycap file location flash:mycap.pcap buffer-size 90
```

Step 2: Confirm that the capture point has been correctly defined by entering:

```
Switch# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 out
   monitor capture mycap match ipv4  any any
   monitor capture mycap file location flash:mycap.pcap buffer-size 90
   monitor capture mycap limit packets 100 duration 60

Switch# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/1, Direction: out
   Status : Inactive
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
   Size of buffer(in MB): 90
  Limit Details:
   Number of Packets to capture: 100
   Packet Capture duration: 60
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
```

Step 3: Launch packet capture by entering:

```
Switch# monitor capture mycap start
A file by the same capture file name already exists, overwrite?[confirm]
Turning on lock-step mode

Switch#
*Oct 14 09:35:32.661: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
```

Note Allow the capture operation stop automatically after the time has elapsed or the packet count has been met. When you see the following message in the output, will know that the capture operation has stopped:

```
*Oct 14 09:36:34.632: %BUFCAP-6-DISABLE_ASYNC: Capture Point mycap disabled. Rea
son : Wireshark Session Ended
```

The mycap.pcap file now contains the captured packets.

Step 4: Display the packets by entering:

```
Switch# show monitor capture file flash:mycap.pcap
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  0.000000    10.1.1.30 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  1.000000    10.1.1.31 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  2.000000    10.1.1.32 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  3.000000    10.1.1.33 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  4.000000    10.1.1.34 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  5.000000    10.1.1.35 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  6.000000    10.1.1.36 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  7.000000    10.1.1.37 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

```
  8.000000    10.1.1.38 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  9.000000    10.1.1.39 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

Step 5: Delete the capture point by entering:

```
Switch# no monitor capture mycap
```

Related Topics

Defining a Capture Point, on page 553
Adding or Modifying Capture Point Parameters, on page 558
Deleting Capture Point Parameters, on page 560
Deleting a Capture Point, on page 562
Activating and Deactivating a Capture Point, on page 563
Clearing the Capture Point Buffer, on page 566
How to Configure Wireshark, on page 553
Capture Points, on page 543
Attachment Points, on page 544

Additional References

Related Documents

Related Topic	Document Title
General Packet Filtering	For general packet filtering, refer to: Display Filter Reference

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
None	-

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Related Topics

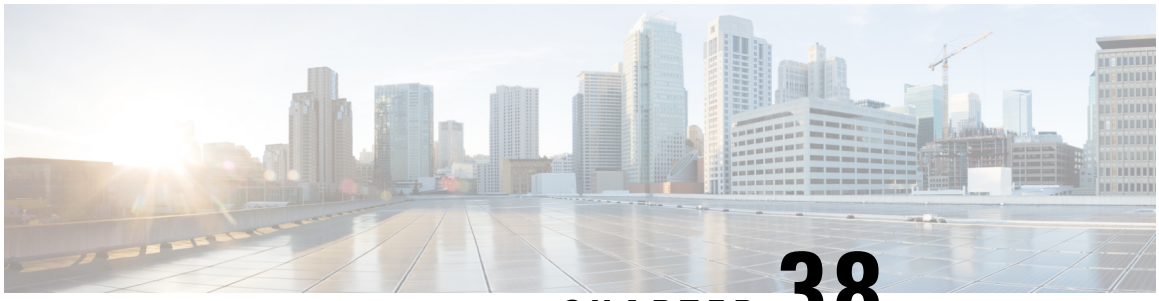
Filters, on page 545

Feature History and Information for WireShark

Release	Modification
Cisco IOS XE 3.3SE	This feature was introduced.

PART IX

QoS



CHAPTER 38

Configuring QoS

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Quality of Service

Before configuring standard QoS, you must have a thorough understanding of these items:

- Standard QoS concepts.
- Wireless concepts and network topologies.
- Classic Cisco IOS QoS.

- Modular QoS CLI (MQC).
- Understanding of QoS implementation.
- The types of applications used and the traffic patterns on your network.
- Traffic characteristics and needs of your network. For example, is the traffic on your network bursty? Do you need to reserve bandwidth for voice and video streams?
- Bandwidth requirements and speed of the network.
- Location of congestion points in the network.

Related Topics

Restrictions for QoS on Wired Targets, on page 629
Restrictions for QoS on Wireless Targets, on page 632

QoS Components

Quality of service (QoS) consists of the following key components:

- Classification— Classification is the process of distinguishing one type of traffic from another based upon access control lists (ACLs), Differentiated Services Code Point (DSCP), Class of Service (CoS), and other factors.
- Marking and mutation— Marking is used on traffic to convey specific information to a downstream device in the network, or to carry information from one interface in a switch to another. When traffic is marked, QoS operations on that traffic can be applied. This can be accomplished directly using the **set** command or through a table map, which takes input values and translates them directly to values on output.
- Shaping and policing— Shaping is the process of imposing a maximum rate of traffic, while regulating the traffic rate in such a way that downstream devices are not subjected to congestion. Shaping in the most common form is used to limit the traffic sent from a physical or logical interface. Policing is used to impose a maximum rate on a traffic class. If the rate is exceeded, then a specific action is taken as soon as the event occurs.
- Queuing — Queueing is used to prevent traffic congestion. Traffic is sent to specific queues for servicing and scheduling based upon bandwidth allocation. Traffic is then scheduled or sent out through the port.
- Bandwidth—Bandwidth allocation determines the available capacity for traffic that is subject to QoS policies.
- Trust— Trust enables traffic to pass through the switch, and the Differentiated Services Code Point (DSCP), precedence, or CoS values coming in from the end points are retained in the absence of any explicit policy configuration.

QoS Terminology

The following terms are used interchangeably in this QoS configuration guide:

- Upstream (direction towards the switch) is the same as ingress.

- Downstream (direction from the switch) is the same as egress.

Note Upstream is wireless to wired. Downstream is wired to wireless. Wireless to wireless has no specific term.

Information About QoS

QoS Overview

By configuring the quality of service (QoS), you can provide preferential treatment to specific types of traffic at the expense of other traffic types. Without QoS, the switch offers best-effort service to each packet, regardless of the packet contents or size. The switch sends the packets without any assurance of reliability, delay bounds, or throughput.

The following are specific features provided by QoS:

- Low latency
- Bandwidth guarantee
- Buffering capabilities and dropping disciplines
- Traffic policing
- Enables the changing of the attribute of the frame or packet header
- Relative services

Related Topics

Restrictions for QoS on Wired Targets, on page 629
Restrictions for QoS on Wireless Targets, on page 632

Modular QoS Command-Line Interface

With the switch, QoS features are enabled through the Modular QoS command-line interface (MQC). The MQC is a command-line interface (CLI) structure that allows you to create traffic policies and attach these policies to interfaces. A traffic policy contains a traffic class and one or more QoS features. A traffic class is used to classify traffic, while the QoS features in the traffic policy determine how to treat the classified traffic. One of the main goals of MQC is to provide a platform-independent interface for configuring QoS across Cisco platforms.

Wireless QoS Overview

Wireless QoS can be configured on the following wireless targets:

- Wireless ports, including all physical ports to which an access point can be associated.
- Radio
- SSID (applicable on a per-radio, per-AP, and per-SSID)

- Client

From Cisco IOS XE Release 3E, marking and policing actions for ingress SSID and client policies are applied at the access point. The SSID and client ingress policies that you configure in the switch are moved to the access point. The access point performs policing and marking actions for each packet. However, the switch selects the QoS policies. Marking and policing of egress SSID and client policies are applied at the switch.

The following table displays how policies are supported for the wireless targets.

Table 34: Wireless Targets Policies Support

Wireless Target	Policies on Wireless Targets Supported	Policies Supported Egress Direction	Policies Supported Ingress Direction
Wireless port	Yes	Yes - user configurable	No
Radio	Yes	Yes - but not configurable by user	No
SSID	Yes	Yes - user configurable	Yes - user configurable
Client	Yes	Yes - user configurable	Yes - user configurable

Note Additional polices that are user configured include multidestination policers and VLANs.

Wireless QoS supports the following features:

- Queuing in the egress direction.
- Policing of wireless traffic
- Marking of wireless traffic.
- Shaping of wireless traffic in the egress direction.
- Approximate Fair Drop (AFD) in the egress direction.
- Mobility support for QoS.
- Compatibility with precious metal QoS policies available on Cisco Unified Wireless Controllers.
- Combination of CLI/Traffic Class (TCLAS) and CLI/snooping.
- Application control (can drop or mark the data traffic) by configuring an AVC QoS client policy.
- Drop action for ingress policies.
- QoS statistics for client and SSID targets in the ingress direction.
- QoS attribute for local profiling policy.
- Hierarchical policies.

QoS and IPv6 for Wireless

The switch supports QoS for both IPv4 and IPv6 traffic, and client policies can now have IPv4 and IPv6 filters.

Wired and Wireless Access Supported Features

The following table describes the supported features for both wired and wireless access.

Table 35: Supported QoS Features for Wired and Wireless Access

Feature	Wired	Wireless
Targets	• Gigabit Ethernet • 10 Gigabit Ethernet • VLAN	• Wireless port (CAPWAP tunnel) • SSID • Client • Radio • CAPWAP multicast tunnel
Configuration Sequence	QoS policy installed using the **service-policy** command.	• When an access point joins the switch, the switch installs a policy on the port. The port policy has a child policy called port_child_policy. • A policy is installed on the radio which has a shaper configured to the radio rate. The default radio policy (which cannot be modified) is attached to the radio. • The default client policies take effect when a WMM client associates, and if admission control is enabled on the radio. • User can modify the port_child_policy to add more classes. • User can attach a user-defined policy at the SSID level. • User can attach a user-defined policy at the client level. • User can configure a port policy. • User can configure an SSID policy. • These policies can then be modified. • The default radio policy (which cannot be modified) is attached to the radio. • Optionally, the user can attach a client policy as required. • The default client policies take effect when a WMM client associates, and if admission control is enabled on the radio.

Feature	Wired	Wireless
Number of queues permitted at port level	Up to 8 queues supported on a port.	Only four queues supported.

Classification mechanism	• DSCP
	• IP precedence
	• CoS
	• QoS-group
	• ACL membership including:
	  • IPv4 ACLs
	  • IPv6 ACLS
	  • MAC ACLs
		• Port level
		  • Ingress: QoS policies not supported on ingress in wireless ports.
		  • Egress: Only DSCP based classification.
		• SSID level
		  • Ingress: DSCP, UP
		  • Egress: DSCP,COS, QoS group
		• Client level
		  • Ingress: ACL, DSCP, UP
		  • Egress: DSCP and COS

Related Topics

Port Policy Format, on page 596

Supported QoS Features on Wireless Targets

This table describes the various features available on wireless targets.

Table 36: QoS Features Available on Wireless Targets

Target	Features	Traffic	Direction Where Policies Are Applicable	Comments
Port	• Port shaper • Priority queuing • Multicast policing	Non-Real Time (NRT), Real Time (RT)	Egress	
Radio	• Shaping	Non-Real Time	Egress	Radio policies are not user configurable.

Target	Features	Traffic	Direction Where Policies Are Applicable	Comments
SSID	• Police • Table map	Non-Real Time, Real Time	Ingress and egress	
	Shaping		Egress	
	BRR		Egress	
	Set actions • Table map • set dscp • set cos		Ingress	You can use set in both class-default and user-defined classes of SSID ingress policies.
	Set actions • Table map • set dscp • set wlan user-priority		Egress	You can define table maps only in the class-default class of an SSID policy.
	Drop		Ingress	
Client	Police	Non-Real Time, Real time	Ingress and egress	For client policies, the following filters are supported: • ACL • DSCP • CoS (only for egress) • WLAN UP • protocol
	Drop		Ingress	
	Set actions • set dscp • set cos		Ingress	
	Set actions • set dscp • set wlan user-priority		Egress	

Related Topics

Configuring Port Policies (GUI), on page 685
Applying or Changing Port Policies (GUI), on page 686
Applying a QoS Policy on a WLAN (GUI), on page 687
Port Policies, on page 596
Port Policy Format, on page 596
Radio Policies, on page 598
Applying an SSID or Client Policy on a WLAN (CLI), on page 653
Configuring SSID Policies (GUI), on page 652
SSID Policies, on page 598
Configuring Client Policies (CLI)
Configuring Client Policies (GUI), on page 642

Client Policies, on page 599

Port Policies

Note Port child policies only apply to wireless ports and not to wired ports on the switch. A wireless port is defined as a port to which APs join. A default port child policy is applied on the switch to the wireless ports at start up.The port shaper rate is limited to 1G

Port shaper specifies the traffic policy applicable between the device and the AP. This is the sum of the radio rates supported on the access point.

The child policy determines the mapping between packets and queues defined by the port-child policy. The child policy can be configured to include voice, video, class-default, and non-client-nrt classes where voice and video are based on DSCP value (which is the outer CAPWAP header DSCP value). The definition of class-default is known to the system as any value other than voice and video DSCP.

The DSCP value is assigned when the packet reaches the port. Before the packet arrives at the port, the SSID policies are applied on the packet. Port child policy also includes multicast percentage for a given port traffic. By default, the port child policy allocates up to 10 percent of the available rate.

Related Topics

Configuring Port Policies (GUI), on page 685
Applying or Changing Port Policies (GUI), on page 686
Applying a QoS Policy on a WLAN (GUI), on page 687
Restrictions for QoS on Wireless Targets, on page 632
Supported QoS Features on Wireless Targets, on page 594
Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic, on page 696

Port Policy Format

This section describes the behavior of the port policies on a switch. The ports on the switch do not distinguish between wired or wireless physical ports. Depending on the kind of device associated to the switch, the policies are applied. For example, when an access point is connected to a switch port, the switch detects it as a wireless device and applies the default hierarchical policy which is in the format of a parent-child policy. This policy is an hierarchical policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suit the QoS configuration. The switch is pre configured with a default class map and a policy map.

Default class map:

```
Class Map match-any non-client-nrt-class
   Match non-client-nrt
```

The above port policy processes all network traffic to the Q3 queue. You can view the class map by executing the **show class-map** command.

Default policy map:

```
Policy Map port_child_policy
    Class non-client-nrt-class
      bandwidth remaining ratio 10
```

Note The class map and policy map listed are system-defined policies and cannot be changed.

The following is the system-defined policy map available on the ports on which wireless devices are associated. The format consists of a parent policy and a service child policy (**port_child_policy**). To customize the policies to suite your network needs, you must configure the port child policy.

```
Policy-map policy_map_name
    Class class-default
         Shape average average_rate
         Service-policy port_child_policy
```

Note The parent policy is system generated and cannot be changed. You must configure the *port_child_policy* policy to suit the QoS requirements on your network.

Depending on the type of traffic in your network, you can configure the port child policy. For example, in a typical wireless network deployment, you can assign specific priorities to voice and video traffic. Here is an example:

```
Policy-map port_child_policy
     Class  voice-policy-name (match dscp ef)
          Priority level 1
          Police (multicast-policer-name-voice) Multicast Policer
    Class video-policy-name (match dscp af41)
        Priority level 2
        Police (multicast-policer-name-video) Multicast Policer
Class non-client-nrt-class traffic(match non-client-nrt)
        Bandwidth remaining ratio (brr-value-nrt-q2)
    Class class-default  (NRT Data)
        Bandwidth remaining ratio (brr-value-q3)
```

In the above port child policy:

- *voice-policy-name*— Refers to the name of the class that specifies rules for the traffic for voice packets. Here the DSCP value is mapped to a value of 46 (represented by the keyword **ef**). The voice traffic is assigned the highest priority of 1.
- *video-policy-name*— Refers to the name of the class that specifies rules for the traffic for video packets. The DSCP value is mapped to a value of 34 (represented by the keyword **af41**).
- *multicast-policer-name-voice*— If you need to configure multicast voice traffic, you can configure policing for the voice class map.
- *multicast-policer-name-video*— If you need to configure multicast video traffic, you can configure policing for the video class map.

In the above sample configuration, all voice and video traffic is directed to the Q0 and Q1 queues, respectively. These queues maintain a strict priority. The packets in Q0 and Q1 are processed in that order. The bandwidth remaining ratios *brr-value-nrt-q2* and *brr-value-q3* are directed to the Q2 and Q3 respectively specified by the class maps and *class-default* and *non-client-nrt*. The processing of packets on Q2 and Q3 are based on a weighted round-robin approach. For example, if the *brr-value-nrtq2* has a value of 90 and *brr-value-nrtq3* is 10, the packets in queue 2 and queue 3 are processed in the ratio of 9:1.

The Cisco 5700 Series Wireless Controller does not contain a default port policy. Physical port policies must be configured for voice and video to function. Because a Cisco 5700 Series Wireless Controller contains six 10-gigabit ports, the policy map must be configured on all ports.

Note The policy must be configured on all of the six physical ports on the controller even if LAG (Link Aggregation/Etherchannel) is configured.

The following basic port policy must be configured on the physical ports. You can add further classification if required:

```
Policy-map <port-policy-name>
  Class voice
      Priority level 1
  class video
     Priority level 2
```

Related Topics

Configuring Port Policies (GUI), on page 685
Applying or Changing Port Policies (GUI), on page 686
Applying a QoS Policy on a WLAN (GUI), on page 687
Restrictions for QoS on Wireless Targets, on page 632
Supported QoS Features on Wireless Targets, on page 594
Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic, on page 696
Wired and Wireless Access Supported Features, on page 593
Policy Maps, on page 608

Radio Policies

The radio policies are system defined and are not user configurable. Radio wireless targets are only applicable in the egress direction.

Radio policies are applicable on a per-radio, per-access point basis. The rate limit on the radios is the practical limit of the AP radio rate. This value is equivalent to the sum of the radios supported by the access point.

The following radios are supported:

- 802.11 a/n
- 802.11 b/n
- 802.11 ac

Related Topics

Restrictions for QoS on Wireless Targets, on page 632
Supported QoS Features on Wireless Targets, on page 594

SSID Policies

You can create QoS policies on SSID BSSID (Basic Service Set Identification) in both the ingress and egress directions. By default, there is no SSID policy. All traffic is transmitted as best effort because the wireless traffic in untrusted. You can configure an SSID policy based on the SSID name. The policy is applicable on a per BSSID.

The types of policies you can create on SSID include marking by using table maps (table-maps), shape rate, and RT1 (Real Time 1) and RT2 (Real Time 2) policiers. If traffic is ingress, you usually configure a marking and policing policy on the SSID. If traffic is downstream, you can configure marking and queuing.

There should be a one-to-one mapping between the policies configured on a port and an SSID. For example, if you configure class voice and class video on the port, you can have a similar policy on the SSID.

The policy on the port is mandatory if you want to preserve the voice and video behavior priority at the port level. Queuing policy is applicable in a downstream direction. When packets arrive from the AP, you can only configure policing and rate limiting.

SSID priorities can be specified by configuring bandwidth remaining ratio. Queuing SSID policies are applied in the egress direction.

Related Topics

Applying an SSID or Client Policy on a WLAN (CLI), on page 653
Configuring SSID Policies (GUI), on page 652
Applying a QoS Policy on a WLAN (GUI), on page 687
Supported QoS Features on Wireless Targets, on page 594
Examples: SSID Policy
Examples: Configuring Downstream SSID Policy, on page 697

Client Policies

Client policies are applicable in the ingress and egress direction. The wireless control module of the switch applies the default client policies when admission control is enabled for WMM clients. When admission control is disabled, there is no default client policy. You can configure policing and marking policies on clients.

Note A client policy can have both IPv4 and IPv6 filters.

You can configure client policies in the following ways:

- Using AAA
- Using the Cisco IOS MQC CLI
  - You can use **service policy client** command in the WLAN configuration.
- Using the default configuration
- Using local policies (native profiling)

Use the **show wireless client mac address** *mac_address* **service-policy** command to display the source of the client policy (for example, local profiling policy, AAA, or CLI). The precedence order of client policies is AAA > local policy > WLAN service client policy CLI > default configuration.

Note If you configured AAA by configuring the unified wireless controller procedure, and using the MQC QoS commands, the policy configuration performed through the MQC QoS commands takes precedence.

Note When applying client policies on a WLAN, you must disable the WLAN before modifying the client policy. SSID policies can be modified even if the WLAN is enabled.

The default client policy is enabled only on Wi-Fi Multimedia (WMM) clients that are admission control (ACM)-enabled.

Policy Chaining

Every packet has a maximum of two applicable policies, first at the client target and second at the SSID target. The client policing action is applied to the packet before the marking action that is specified in the client policy. After the client policing and marking actions are applied to the packet, the SSID policy action is applied to the updated packet. If no custom policies are specified, the system trust configuration is applied to the packet. Egress trust is based on DSCP, and ingress trust is based on WLAN user priority.

Related Topics

Configuring Client Policies (CLI)
Configuring Client Policies (GUI), on page 642
Applying a QoS Policy on a WLAN (GUI), on page 687
Supported QoS Features on Wireless Targets, on page 594
Examples: Client Policies, on page 699

Hierarchical QoS

The switch supports hierarchical QoS (HQoS). HQoS allows you to perform:

- Hierarchical classification— Traffic classification is based upon other classes.
- Hierarchical policing—The process of having the policing configuration at multiple levels in a hierarchical policy.
- Hierarchical shaping—Shaping can also be configured at multiple levels in the hierarchy.

Note Hierarchical shaping is only supported for the port shaper, where for the parent you only have a configuration for the class default, and the only action for the class default is shaping.

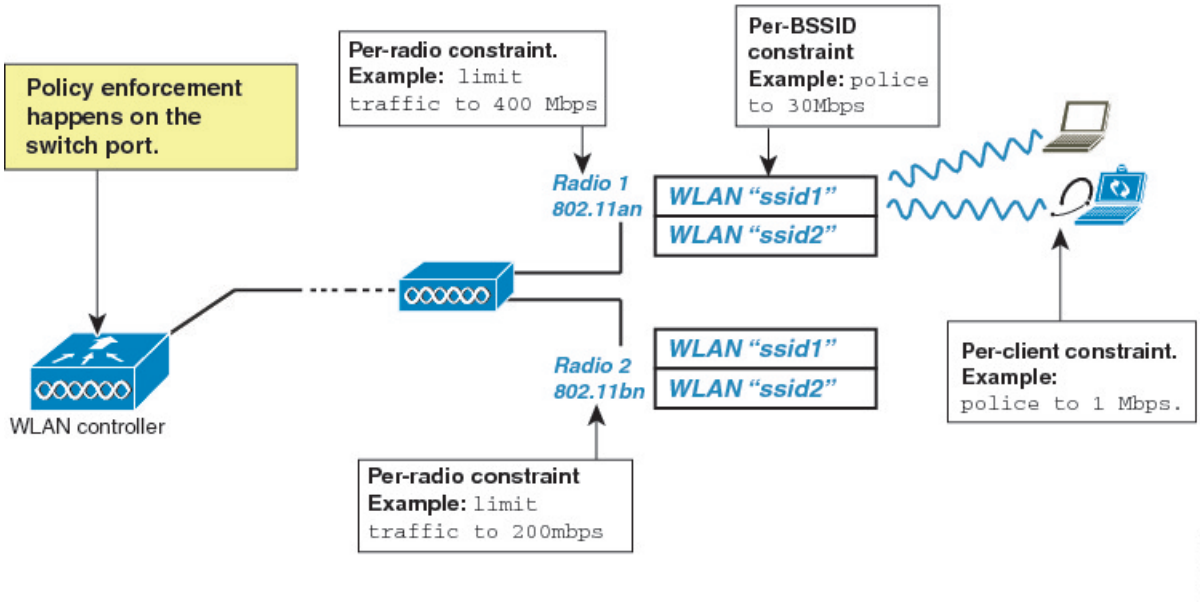
Related Topics

Examples: Hierarchical Classification, on page 694
Examples: Hierarchical Policy Configuration, on page 694

Hierarchical Wireless QoS

The switch supports hierarchical QoS for wireless targets. Hierarchical QoS policies are applicable on port, radio, SSID, and client. QoS policies configured on the device (including marking, shaping, policing) can be applied across the targets. If the network contains non-realtime traffic, the non-realtime traffic is subject to approximate fair drop. Hierarchy refers to the process of application of the various QoS policies on the packets arriving to the device. You can configure policing in both the parent and child policies.

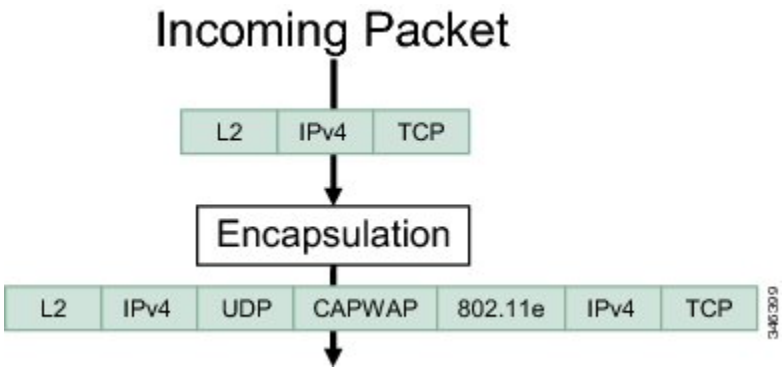
Note For hierarchical client and SSID policies, you only configure marking either in the parent or child policy.



Wireless Packet Format

Figure 38: Wireless Packet Path in the Egress Direction during First Pass

This figure displays the wireless packet flow and encapsulation used in hierarchical wireless QoS. The incoming packet enters the switch. The switch encapsulates this incoming packet and adds the 802.11e and CAPWAP headers.



Hierarchical AFD

Approximate Fair Dropping (AFD) is a feature provided by the QoS infrastructure in Cisco IOS. For wireless targets, AFD can be configured on SSID (via shaping) and clients (via policing). AFD shaping rate is only applicable for downstream direction. Unicast real-time traffic is not subjected to AFD drops.

QoS Implementation

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When you configure the QoS feature, you can select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

The QoS implementation is based on the Differentiated Services (Diff-Serv) architecture, a standard from the Internet Engineering Task Force (IETF). This architecture specifies that each packet is classified upon entry into the network.

The classification is carried in the IP packet header, using 6 bits from the deprecated IP type of service (ToS) field to carry the classification (*class*) information. Classification can also be carried in the Layer 2 frame.

Figure 39: QoS Classification Layers in Frames and Packets

The special bits in the Layer 2 frame or a Layer 3 packet are shown in the following

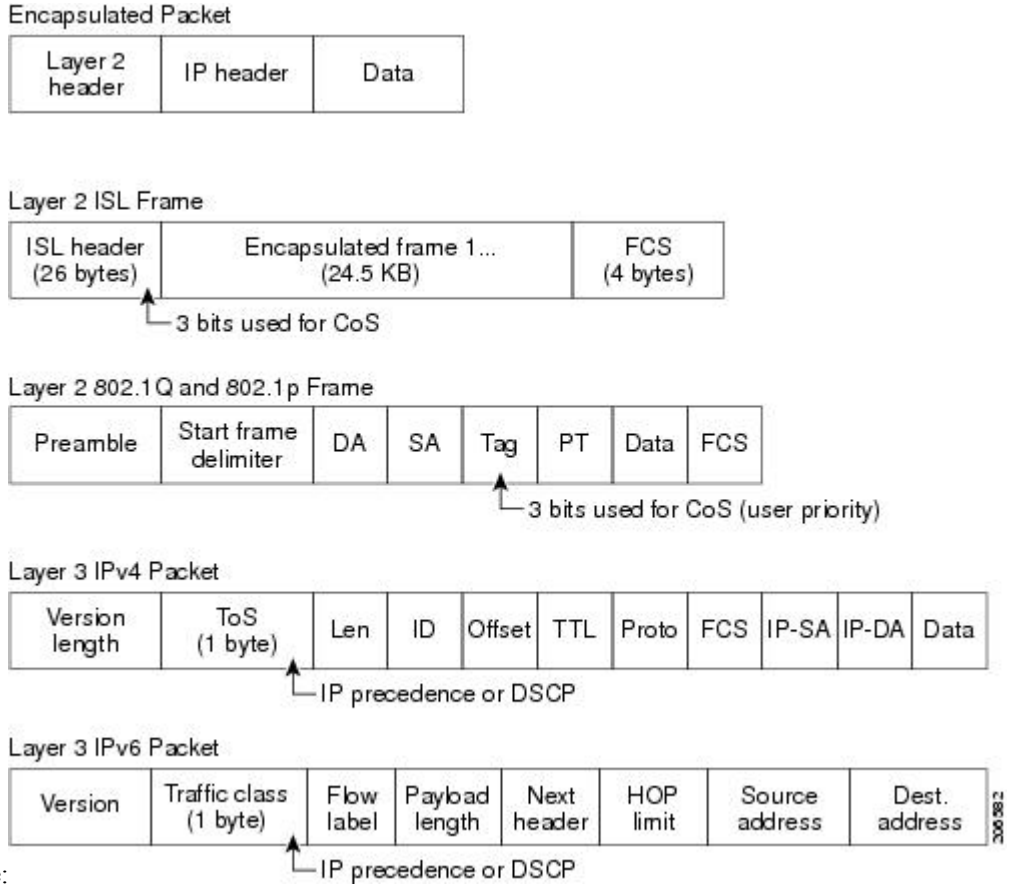


figure:

Related Topics

Restrictions for QoS on Wired Targets, on page 629
Restrictions for QoS on Wireless Targets, on page 632

Layer 2 Frame Prioritization Bits

Layer 2 Inter-Switch Link (ISL) frame headers have a 1-byte User field that carries an IEEE 802.1p class of service (CoS) value in the three least-significant bits. On ports configured as Layer 2 ISL trunks, all traffic is in ISL frames.

Layer 2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value in the three most-significant bits, which are called the User Priority bits. On ports configured as Layer 2 802.1Q trunks, all traffic is in 802.1Q frames except for traffic in the native VLAN.

Other frame types cannot carry Layer 2 CoS values.

Layer 2 CoS values range from 0 for low priority to 7 for high priority.

Layer 3 Packet Prioritization Bits

Layer 3 IP packets can carry either an IP precedence value or a Differentiated Services Code Point (DSCP) value. QoS supports the use of either value because DSCP values are backward-compatible with IP precedence values.

IP precedence values range from 0 to 7. DSCP values range from 0 to 63.

End-to-End QoS Solution Using Classification

All switches and routers that access the Internet rely on the class information to provide the same forwarding treatment to packets with the same class information and different treatment to packets with different class information. The class information in the packet can be assigned by end hosts or by switches or routers along the way, based on a configured policy, detailed examination of the packet, or both. Detailed examination of the packet is expected to occur closer to the edge of the network, so that the core switches and routers are not overloaded with this task.

Switches and routers along the path can use the class information to limit the amount of resources allocated per traffic class. The behavior of an individual device when handling traffic in the Diff-Serv architecture is called per-hop behavior. If all devices along a path provide a consistent per-hop behavior, you can construct an end-to-end QoS solution.

Implementing QoS in your network can be a simple task or complex task and depends on the QoS features offered by your internetworking devices, the traffic types and patterns in your network, and the granularity of control that you need over incoming and outgoing traffic.

Packet Classification

Packet classification is the process of identifying a packet as belonging to one of several classes in a defined policy, based on certain criteria. The Modular QoS CLI (MQC) is a policy-class based language. The policy class language is used to define the following:

- Class-map template with one or several match criteria
- Policy-map template with one or several classes associated to the policy map

The policy map template is then associated to one or several interfaces on the switch.

Packet classification is the process of identifying a packet as belonging to one of the classes defined in the policy map. The process of classification will exit when the packet being processed matches a specific filter in a class. This is referred to as first-match exit. If a packet matches multiple classes in a policy, irrespective

of the order of classes in the policy map, it would still exit the classification process after matching the first class.

If a packet does not match any of the classes in the policy, it would be classified into the default class in the policy. Every policy map has a default class, which is a system-defined class to match packets that do not match any of the user-defined classes.

Packet classification can be categorized into the following types:

- Classification based on information that is propagated with the packet
- Classification based on information that is switch specific
- Hierarchical classification

Classification Based on Information That is Propagated with the Packet

Classification that is based on information that is part of the packet and propagated either end-to-end or between hops, typically includes the following:

- Classification based on Layer 3 or 4 headers
- Classification based on Layer 2 information

Classification Based on Layer 3 or Layer 4 Header

This is the most common deployment scenario. Numerous fields in the Layer 3 and Layer 4 headers can be used for packet classification.

At the most granular level, this classification methodology can be used to match an entire flow. For this deployment type, an access control list (ACLs) can be used. ACLs can also be used to match based on various subsets of the flow (for example, source IP address only, or destination IP address only, or a combination of both).

Classification can also be done based on the precedence or DSCP values in the IP header. The IP precedence field is used to indicate the relative priority with which a particular packet needs to be handled. It is made up of three bits in the IP header's type of service (ToS) byte.

The following table shows the different IP precedence bit values and their names.

Note IP precedence is not supported for wireless QoS.

Table 37: IP Precedence Values and Names

IP Precedence Value	IP Precedence Bits	IP Precedence Names
0	000	Routine
1	001	Priority
2	010	Immediate
3	011	Flash
4	100	Flash Override
5	101	Critical

IP Precedence Value	IP Precedence Bits	IP Precedence Names
6	110	Internetwork control
7	111	Network control

Note All routing control traffic in the network uses IP precedence value 6 by default. IP precedence value 7 also is reserved for network control traffic. Therefore, the use of IP precedence values 6 and 7 is not recommended for user traffic.

The DSCP field is made up of 6 bits in the IP header and is being standardized by the Internet Engineering Task Force (IETF) Differentiated Services Working Group. The original ToS byte contained the DSCP bits has been renamed the DSCP byte. The DSCP field is part of the IP header, similar to IP precedence. The DSCP field is a super set of the IP precedence field. Therefore, the DSCP field is used and is set in ways similar to what was described with respect to IP precedence.

Note The DSCP field definition is backward-compatible with the IP precedence values.

Classification Based on Layer 2 Header

A variety of methods can be used to perform classification based on the Layer 2 header information. The most common methods include the following:

- MAC address-based classification (only for access groups)—Classification is based upon the source MAC address (for policies in the input direction) and destination MAC address (for policies in the output direction).
- Class-of-Service—Classification is based on the 3 bits in the Layer 2 header based on the IEEE 802.1p standard. This usually maps to the ToS byte in the IP header.
- VLAN ID—Classification is based on the VLAN ID of the packet.

Note Some of these fields in the Layer 2 header can also be set using a policy.

Classification Based on Information that is Device Specific (QoS Groups)

The switch also provides classification mechanisms that are available where classification is not based on information in the packet header or payload.

At times you might be required to aggregate traffic coming from multiple input interfaces into a specific class in the output interface. For example, multiple customer edge routers might be going into the same access switch on different interfaces. The service provider might want to police all the aggregate voice traffic going into the core to a specific rate. However, the voice traffic coming in from the different customers could have a different ToS settings. QoS group-based classification is a feature that is useful in these scenarios.

Policies configured on the input interfaces set the QoS group to a specific value, which can then be used to classify packets in the policy enabled on output interface.

The QoS group is a field in the packet data structure internal to the switch. It is important to note that a QoS group is an internal label to the switch and is not part of the packet header.

Hierarchical Classification

The switch permits you to perform a classification based on other classes. Typically, this action may be required when there is a need to combine the classification mechanisms (that is, filters) from two or more classes into a single class map.

QoS Wired Model

To implement QoS, the switch must perform the following tasks:

- Traffic classification—Distinguishes packets or flows from one another.
- Traffic marking and policing—Assigns a label to indicate the given quality of service as the packets move through the switch , and then make the packets comply with the configured resource usage limits.
- Queuing and scheduling—Provides different treatment in all situations where resource contention exists.
- Shaping—Ensures that traffic sent from the switch meets a specific traffic profile.

Ingress Port Activity

The following activities occur at the ingress port of the switch:

- Classification—Classifying a distinct path for a packet by associating it with a QoS label. For example, the switch maps the CoS or DSCP in the packet to a QoS label to distinguish one type of traffic from another. The QoS label that is generated identifies all future QoS actions to be performed on this packet.
- Policing—Policing determines whether a packet is in or out of profile by comparing the rate of the incoming traffic to the configured policer. The policer limits the bandwidth consumed by a flow of traffic. The result is passed to the marker.
- Marking—Marking evaluates the policer and configuration information for the action to be taken when a packet is out of profile and determines what to do with the packet (pass through a packet without modification, mark down the QoS label in the packet, or drop the packet).

Note Applying polices on the wireless ingress port is not supported on the switch.

Egress Port Activity

The following activities occur at the egress port of the switch:

- Policing—Policing determines whether a packet is in or out of profile by comparing the rate of the incoming traffic to the configured policer. The policer limits the bandwidth consumed by a flow of traffic. The result is passed to the marker.
- Marking—Marking evaluates the policer and configuration information for the action to be taken when a packet is out of profile and determines what to do with the packet (pass through a packet without modification, mark down the QoS label in the packet, or drop the packet).

- Queueing—Queueing evaluates the QoS packet label and the corresponding DSCP or CoS value before selecting which of the egress queues to use. Because congestion can occur when multiple ingress ports simultaneously send data to an egress port, Weighted Tail Drop (WTD) differentiates traffic classes and subjects the packets to different thresholds based on the QoS label. If the threshold is exceeded, the packet is dropped.

Classification

Classification is the process of distinguishing one kind of traffic from another by examining the fields in the packet. Classification is enabled only if QoS is enabled on the switch. By default, QoS is enabled on the switch.

During classification, the switch performs a lookup and assigns a QoS label to the packet. The QoS label identifies all QoS actions to be performed on the packet and from which queue the packet is sent.

Access Control Lists

You can use IP standard, IP extended, or Layer 2 MAC ACLs to define a group of packets with the same characteristics (class). You can also classify IP traffic based on IPv6 ACLs.

In the QoS context, the permit and deny actions in the access control entries (ACEs) have different meanings from security ACLs:

- If a match with a permit action is encountered (first-match principle), the specified QoS-related action is taken.
- If a match with a deny action is encountered, the ACL being processed is skipped, and the next ACL is processed.

Note Deny action is supported in Cisco IOS Release 3.7.4E and later releases.

- If no match with a permit action is encountered and all the ACEs have been examined, no QoS processing occurs on the packet, and the switch offers best-effort service to the packet.
- If multiple ACLs are configured on a port, the lookup stops after the packet matches the first ACL with a permit action, and QoS processing begins.

Note When creating an access list, note that by default the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.

After a traffic class has been defined with the ACL, you can attach a policy to it. A policy might contain multiple classes with actions specified for each one of them. A policy might include commands to classify the class as a particular aggregate (for example, assign a DSCP) or rate-limit the class. This policy is then attached to a particular port on which it becomes effective.

You implement IP ACLs to classify IP traffic by using the **access-list** global configuration command; you implement Layer 2 MAC ACLs to classify non-IP traffic by using the **mac access-list extended** global configuration command.

Class Maps

A class map is a mechanism that you use to name a specific traffic flow (or class) and isolate it from all other traffic. The class map defines the criteria used to match against a specific traffic flow to further classify it. The criteria can include matching the access group defined by the ACL or matching a specific list of DSCP or IP precedence values. If you have more than one type of traffic that you want to classify, you can create another class map and use a different name. After a packet is matched against the class-map criteria, you further classify it through the use of a policy map.

You create a class map by using the **class-map** global configuration command or the **class** policy-map configuration command. You should use the **class-map** command when the map is shared among many ports. When you enter the **class-map** command, the switch enters the class-map configuration mode. In this mode, you define the match criterion for the traffic by using the **match** class-map configuration command.

You can create a default class by using the **class class-default** policy-map configuration command. The default class is system-defined and cannot be configured. Unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is treated as default traffic.

Related Topics

Creating a Traffic Class (CLI), on page 635
Examples: Classification by Access Control Lists, on page 692

Policy Maps

A policy map specifies which traffic class to act on. Actions can include the following:

- Setting a specific DSCP or IP precedence value in the traffic class
- Setting a CoS value in the traffic class
- Setting a QoS group
- Setting a wireless LAN (WLAN) value in the traffic class
- Specifying the traffic bandwidth limitations and the action to take when the traffic is out of profile

Before a policy map can be effective, you must attach it to a port.

You create and name a policy map using the **policy-map** global configuration command. When you enter this command, the switch enters the policy-map configuration mode. In this mode, you specify the actions to take on a specific traffic class by using the **class** or **set** policy-map configuration and policy-map class configuration commands.

The policy map can also be configured using the **police** and **bandwidth** policy-map class configuration commands, which define the policer, the bandwidth limitations of the traffic, and the action to take if the limits are exceeded. In addition, the policy-map can further be configured using the **priority** policy-map class configuration command, to schedule priority for the class or the queueing policy-map class configuration commands, **queue-buffers** and **queue-limit**.

To enable the policy map, you attach it to a port by using the **service-policy** interface configuration command.

Note You cannot configure both **priority** and **set** for a policy map. If both these commands are configured for a policy map, and when the policy map is applied to an interface, error messages are displayed. The following example shows this restriction:

```
Switch# configure terminal
Switch(config)# class-map cmap
Switch(config-cmap)# exit
Switch(config)# class-map classmap1
Switch(config-cmap)# exit
Switch(config)# policy-map pmap
Switch(config-pmap)# class cmap
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classmap1
Switch(config-pmap-c)# set
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1/1
Switch(config-if)# service-policy output pmap

Non-queuing action only is unsupported in a queuing policy!!!
%QOS-6-POLICY_INST_FAILED:
Service policy installation failed
```

Related Topics

Creating a Traffic Policy (CLI), on page 638
Port Policy Format, on page 596

Policy Map on Physical Port

You can configure a nonhierarchical policy map on a physical port that specifies which traffic class to act on. Actions can include setting a specific DSCP or IP precedence value in the traffic class, specifying the traffic bandwidth limitations for each matched traffic class (policer), and taking action when the traffic is out of profile (marking).

A policy map also has these characteristics:

- A policy map can contain multiple class statements, each with different match criteria and policers.
- A policy map can contain a predefined default traffic class explicitly placed at the end of the map.

  When you configure a default traffic class by using the **class class-default** policy-map configuration command, unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is treated as the default traffic class (**class-default**).
- A separate policy-map class can exist for each type of traffic received through a port.

Related Topics

Attaching a Traffic Policy to an Interface (CLI), on page 650

Policy Map on VLANs

The switch supports a VLAN QoS feature that allows the user to perform QoS treatment at the VLAN level (classification and QoS actions) using the incoming frame's VLAN information. In VLAN-based QoS, a service policy is applied to an SVI interface. All physical interfaces belonging to a VLAN policy map then need to be programmed to refer to the VLAN-based policy maps instead of the port-based policy map.

Although the policy map is applied to the VLAN SVI, any policing (rate-limiting) action can only be performed on a per-port basis. You cannot configure the policer to take account of the sum of traffic from a number of physical ports. Each port needs to have a separate policer governing the traffic coming into that port.

Related Topics

Classifying, Policing, and Marking Traffic on SVIs by Using Policy Maps (CLI), on page 657
Examples: Policer VLAN Configuration, on page 704

Wireless QoS Multicast

You can configure multicast policing rate at the port level.

There are two modes of a multicast configuration in the Cisco 5700 Series Wireless Controller:

- multicast-unicast mode—Multicast traffic is copied as unicast traffic to the APs. QoS on multicast traffic when multicast-unicast mode is not supported on the Cisco 5700 Series Wireless Controller.
- multicast-multicast mode—The controller sends the traffic to the multicast group. The APs in the multicast group then receive the multicast traffic.

Related Topics

Configuring QoS Policies for Multicast Traffic (CLI), on page 685
Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic, on page 696

Policing

After a packet is classified and has a DSCP-based, CoS-based, or QoS-group label assigned to it, the policing and marking process can begin.

Policing involves creating a policer that specifies the bandwidth limits for the traffic. Packets that exceed the limits are *out of profile* or *nonconforming*. Each policer decides on a packet-by-packet basis whether the packet is in or out of profile and specifies the actions on the packet. These actions, carried out by the marker, include passing through the packet without modification, dropping the packet, or modifying (marking down) the assigned DSCP or CoS value of the packet and allowing the packet to pass through.

To avoid out-of-order packets, both conform and nonconforming traffic typically exit the same queue.

Note All traffic, regardless of whether it is bridged or routed, is subjected to a policer, if one is configured. As a result, bridged packets might be dropped or might have their DSCP or CoS fields modified when they are policed and marked.

You can only configure policing on a physical port.

After you configure the policy map and policing actions, attach the policy to an ingress port or SVI by using the **service-policy** interface configuration command.

Related Topics

Configuring Police (CLI), on page 672
Examples: Policing Action Configuration, on page 703

Token-Bucket Algorithm

Policing uses a token-bucket algorithm. As each frame is received by the switch, a token is added to the bucket. The bucket has a hole in it and leaks at a rate that you specify as the average traffic rate in bits per second. Each time a token is added to the bucket, the switch verifies that there is enough room in the bucket. If there is not enough room, the packet is marked as nonconforming, and the specified policer action is taken (dropped or marked down).

How quickly the bucket fills is a function of the bucket depth (burst-byte), the rate at which the tokens are removed (rate-bps), and the duration of the burst above the average rate. The size of the bucket imposes an upper limit on the burst length and limits the number of frames that can be transmitted back-to-back. If the burst is short, the bucket does not overflow, and no action is taken against the traffic flow. However, if a burst is long and at a higher rate, the bucket overflows, and the policing actions are taken against the frames in that burst.

You configure the bucket depth (the maximum burst that is tolerated before the bucket overflows) by using the burst-byte option of the **police** policy-map class configuration command. You configure how fast (the average rate) that the tokens are removed from the bucket by using the rate option of the **police** policy-map class configuration command.

Related Topics

Configuring Police (CLI), on page 672
Examples: Policing Action Configuration, on page 703
Examples: Policing Units, on page 704

Marking

Marking is used to convey specific information to a downstream device in the network, or to carry information from one interface in a switch to another.

Marking can be used to set certain field/bits in the packet headers, or marking can also be used to set certain fields in the packet structure that is internal to the switch. Additionally, the marking feature can be used to define mapping between fields. The following marking methods are available for QoS:

- Packet header
- Device (switch)) specific information
- Table maps

Packet Header Marking

Marking on fields in the packet header can be classified into two general categories:

- IPv4/v6 header bit marking
- Layer 2 header bit marking

The marking feature at the IP level is used to set the precedence or the DSCP in the IP header to a specific value to get a specific per-hop behavior at the downstream device (switch or router), or it can also be used to aggregate traffic from different input interfaces into a single class in the output interface. The functionality is currently supported on both the IPv4 and IPv6 headers.

Marking in the Layer 2 headers is typically used to influence dropping behavior in the downstream devices (switch or router). It works in tandem with the match on the Layer 2 headers. The bits in the Layer 2 header that can be set using a policy map are class of service.

Switch Specific Information Marking

This form of marking includes marking of fields in the packet data structure that are not part of the packets header, so that the marking can be used later in the data path. This is not propagated between the switches. Marking of QoS-group falls into this category. This form of marking is only supported in policies that are enabled on the input interfaces. The corresponding matching mechanism can be enabled on the output interfaces on the same switch and an appropriate QoS action can be applied.

Table Map Marking

Note QoS marking is not supported on the 802.11ac Wave 2 APs. This is because table-maps used for QoS marking are not supported on the 802.11ac Wave 2 APs.

Table map marking enables the mapping and conversion from one field to another using a conversion table. This conversion table is called a table map.

Depending upon the table map attached to an interface, CoS, DSCP, and UP values (UP specific to wireless packets) of the packet are rewritten. The switch allows configuring both ingress table map policies and egress table map policies.

As an example, a table map can be used to map the Layer 2 CoS setting to a precedence value in Layer 3. This feature enables combining multiple **set** commands into a single table, which indicates the method to perform the mapping. This table can be referenced in multiple policies, or multiple times in the same policy.

The following table shows the currently supported forms of mapping:

Table 38: Packet-Marking Types Used for Establishing a To-From Relationship

The To Packet-Marking Type	The From Packet-Marking Type
Precedence	CoS
Precedence	QoS Group
DSCP	CoS
DSCP	QoS Group
CoS	Precedence
CoS	DSCP
QoS Group	Precedence
QoS Group	DSCP

A table map-based policy supports the following capabilities:

- Mutation—You can have a table map that maps from one DSCP value set to another DSCP value set, and this can be attached to an egress port.
- Rewrite—Packets coming in are rewritten depending upon the configured table map.
- Mapping—Table map based policies can be used instead of set policies.

The following steps are required for table map marking:

1. Define the table map—Use the **table-map** global configuration command to map the values. The table does not know of the policies or classes within which it will be used. The default command in the table map is used to indicate the value to be copied into the to field when there is no matching from field.
2. Define the policy map—You must define the policy map where the table map will be used.
3. Associate the policy to an interface.

Note A table map policy on an input port changes the trust setting of that port to the from type of qos-marking.

Related Topics

Configuring Table Maps (CLI), on page 660
Examples: Table Map Marking Configuration, on page 706

Traffic Conditioning

To support QoS in a network, traffic entering the service provider network needs to be policed on the network boundary routers to ensure that the traffic rate stays within the service limit. Even if a few routers at the network boundary start sending more traffic than what the network core is provisioned to handle, the increased traffic load leads to network congestion. The degraded performance in the network makes it difficult to deliver QoS for all the network traffic.

Traffic policing functions (using the police feature) and shaping functions (using the traffic shaping feature) manage the traffic rate, but differ in how they treat traffic when tokens are exhausted. The concept of tokens comes from the token bucket scheme, a traffic metering function.

Note When running QoS tests on network traffic, you may see different results for the shaper and policing data. Network traffic data from shaping provides more accurate results.

This table compares the policing and shaping functions.

Table 39: Comparison Between Policing and Shaping Functions

Policing Function	Shaping Function
Sends conforming traffic up to the line rate and allows bursts.	Smooths traffic and sends it out at a constant rate.

Policing Function	Shaping Function
When tokens are exhausted, action is taken immediately.	When tokens are exhausted, it buffers packets and sends them out later, when tokens are available. A class with shaping has a queue associated with it which will be used to buffer the packets.
Policing has multiple units of configuration – in bits per second, packets per second and cells per second.	Shaping has only one unit of configuration - in bits per second.
Policing has multiple possible actions associated with an event, marking and dropping being example of such actions.	Shaping does not have the provision to mark packets that do not meet the profile.
Works for both input and output traffic.	Implemented for output traffic only.
Transmission Control Protocol (TCP) detects the line at line speed but adapts to the configured rate when a packet drop occurs by lowering its window size.	TCP can detect that it has a lower speed line and adapt its retransmission timer accordingly. This results in less scope of retransmissions and is TCP-friendly.

Policing

The QoS policing feature is used to impose a maximum rate on a traffic class. The QoS policing feature can also be used with the priority feature to restrict priority traffic. If the rate is exceeded, then a specific action is taken as soon as the event occurs. The rate (committed information rate [CIR] and peak information rate [PIR]) and the burst parameters (conformed burst size [B_c] and extended burst size [B_e]) are all configured in bytes per second.

The following policing forms or policers are supported for QoS:

- Single-rate two-color policing
- Dual-rate three-color policing

Note Single-rate three-color policing is not supported.

Single-Rate Two-Color Policing

Single-rate two-color policer is the mode in which you configure only a CIR and a B_c.

The B_c is an optional parameter, and if it is not specified it is computed by default. In this mode, when an incoming packet has enough tokens available, the packet is considered to be conforming. If at the time of packet arrival, enough tokens are not available within the bounds of B_c, the packet is considered to have exceeded the configured rate.

Note For information about the token-bucket algorithm, see Token-Bucket Algorithm, on page 611.

Related Topics

Configuring Police (CLI), on page 672

Examples: Single-Rate Two-Color Policing Configuration, on page 705

Dual-Rate Three-Color Policing

With the dual rate policer, the switch supports only color-blind mode. In this mode, you configure a committed information rate (CIR) and a peak information rate (PIR). As the name suggests, there are two token buckets in this case, one for the peak rate, and one for the conformed rate.

Note For information about the token-bucket algorithm, see Token-Bucket Algorithm, on page 611.

In the color-blind mode, the incoming packet is first checked against the peak rate bucket. If there are not enough tokens available, the packet is said to violate the rate. If there are enough tokens available, then the tokens in the conformed rate buckets are checked to determine if there are enough tokens available. The tokens in the peak rate bucket are decremented by the size of the packet. If it does not have enough tokens available, the packet is said to have exceeded the configured rate. If there are enough tokens available, then the packet is said to conform, and the tokens in both the buckets are decremented by the size of the packet.

The rate at which tokens are replenished depends on the packet arrival. Assume that a packet comes in at time T1 and the next one comes in at time T2. The time interval between T1 and T2 determines the number of tokens that need to be added to the token bucket. This is calculated as:

Time interval between packets (T2-T1) * CIR)/8 bytes

Related Topics

Configuring Police (CLI), on page 672
Examples: Dual-Rate Three-Color Policing Configuration, on page 705

Shaping

Shaping is the process of imposing a maximum rate of traffic, while regulating the traffic rate in such a way that the downstream switches and routers are not subjected to congestion. Shaping in the most common form is used to limit the traffic sent from a physical or logical interface.

Shaping has a buffer associated with it that ensures that packets which do not have enough tokens are buffered as opposed to being immediately dropped. The number of buffers available to the subset of traffic being shaped is limited and is computed based on a variety of factors. The number of buffers available can also be tuned using specific QoS commands. Packets are buffered as buffers are available, beyond which they are dropped.

Class-Based Traffic Shaping

The switch uses class-based traffic shaping. This shaping feature is enabled on a class in a policy that is associated to an interface. A class that has shaping configured is allocated a number of buffers to hold the packets that do not have tokens. The buffered packets are sent out from the class using FIFO. In the most common form of usage, class-based shaping is used to impose a maximum rate for an physical interface or logical interface as a whole. The following shaping forms are supported in a class:

- Average rate shaping
- Hierarchical shaping

Shaping is implemented using a token bucket. The values of CIR, B_c and B_e determine the rate at which the packets are sent out and the rate at which the tokens are replenished.

Note For information about the token-bucket algorithm, see Token-Bucket Algorithm, on page 611.

Average Rate Shaping

You use the **shape average** policy-map class command to configure average rate shaping.

This command configures a maximum bandwidth for a particular class. The queue bandwidth is restricted to this value even though the port has more bandwidth available. The switch supports configuring shape average by either a percentage or by a target bit rate value.

Related Topics

Configuring Shaping (CLI), on page 682
Examples: Average Rate Shaping Configuration, on page 701

Hierarchical Shaping

Shaping can also be configured at multiple levels in a hierarchy. This is accomplished by creating a parent policy with shaping configured, and then attaching child policies with additional shaping configurations to the parent policy.

There are two supported types of hierarchical shaping:

- Port shaper
- User-configured shaping

The port shaper uses the class default and the only action permitted in the parent is shaping. The queueing action is in the child with the port shaper. With the user configured shaping, you cannot have queueing action in the child.

Related Topics

Configuring Shaping (CLI), on page 682

Queueing and Scheduling

The switch uses both queueing and scheduling to help prevent traffic congestion. The switch supports the following queueing and scheduling features:

- Bandwidth
- Weighted Tail Drop
- Priority queues
- Queue buffers

When you define a queuing policy on a port, control packets are mapped to the best priority queue with the highest threshold. Control packets queue mapping works differently in the following scenarios:

- Without a quality of service (QoS) policy—If no QoS policy is configured, control packets with DSCP values 16, 24, 48, and 56 are mapped to queue 0 with the highest threshold of threshold2.
- With an user-defined policy—An user-defined queuing policy configured on egress ports can affect the default priority queue setting on control packets.

Control traffic is redirected to the best queue based on the following rules:

1. If defined in a user policy, the highest- level priority queue is always chosen as the best queue.
2. In the absence of a priority queue, Cisco IOS software selects queue 0 as the best queue. When the software selects queue 0 as the best queue, you must define the highest bandwidth to this queue to get the best QoS treatment to the control plane traffic.
3. If thresholds are not configured on the best queue, Cisco IOS software assigns control packets with Differentiated Services Code Point (DSCP) values 16, 24, 48, and 56 are mapped to threshold2 and reassigns the rest of the control traffic in the best queue to threshold1.

If a policy is not configured explicitly for control traffic, the Cisco IOS software maps all unmatched control traffic to the best queue with threshold2, and the matched control traffic is mapped to the queue as configured in the policy.

Note To provide proper QoS for Layer 3 packets, you must ensure that packets are explicitly classified into appropriate queues. When the software detects DSCP values in the default queue, then it automatically reassigns this queue as the best queue.

Bandwidth

The switch supports the following bandwidth configurations:

- Bandwidth percent
- Bandwidth remaining ratio

Related Topics

Configuring Bandwidth (CLI), on page 670

Bandwidth Percent

You can use the **bandwidth percent** policy-map class command to allocate a minimum bandwidth to a particular class. The total sum cannot exceed 100 percent and in case the total sum is less than 100 percent, then the rest of the bandwidth is divided equally among all bandwidth queues.

Note A queue can oversubscribe bandwidth in case the other queues do not utilize the entire port bandwidth.

You cannot mix bandwidth types on a policy map. For example, you cannot configure bandwidth in a single policy map using both a bandwidth percent and in kilobits per second.

Bandwidth Remaining Ratio

You use the **bandwidth remaining ratio** policy-map class command to create a ratio for sharing unused bandwidth in specified queues. Any unused bandwidth will be used by these specific queues in the ratio that is specified by the configuration. Use this command when the **priority** command is also used for certain queues in the policy.

When you assign ratios, the queues will be assigned certain weights which are inline with these ratios.

You can specify ratios using a range from 0 to 100. For example, you can configure a bandwidth remaining ration of 2 on one class, and another queue with a bandwidth remaining ratio of 4 on another class. The bandwidth remaining ratio of 4 will be scheduled twice as often as the bandwidth remaining ratio of 2.

The total bandwidth ratio allocation for the policy can exceed 100. For example, you can configure a queue with a bandwidth remaining ratio of 50, and another queue with a bandwidth remaining ratio of 100.

Weighted Tail Drop

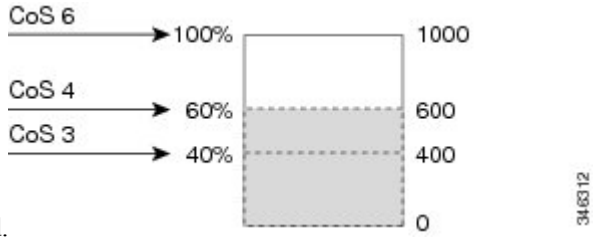
The switch egress queues use an enhanced version of the tail-drop congestion-avoidance mechanism called weighted tail drop (WTD). WTD is implemented on queues to manage the queue lengths and to provide drop precedences for different traffic classifications.

As a frame is enqueued to a particular queue, WTD uses the frame's assigned QoS label to subject it to different thresholds. If the threshold is exceeded for that QoS label (the space available in the destination queue is less than the size of the frame), the switch drops the frame.

Each queue has three configurable threshold values. The QoS label determines which of the three threshold values is subjected to the frame.

Figure 40: WTD and Queue Operation

The following figure shows an example of WTD operating on a queue whose size is 1000 frames. Three drop percentages are configured: 40 percent (400 frames), 60 percent (600 frames), and 100 percent (1000 frames). These percentages indicate that up to 400 frames can be queued at the 40-percent threshold, up to 600 frames at the 60-percent threshold, and up to 1000 frames at the 100-percent threshold.



In the example, CoS value 6 has a greater importance than the other CoS values, and is assigned to the 100-percent drop threshold (queue-full state). CoS values 4 is assigned to the 60-percent threshold, and CoS values 3 is assigned to the 40-percent threshold. All of these threshold values are assigned using the **queue-limit cos** command.

Assuming the queue is already filled with 600 frames, and a new frame arrives. It contains CoS value 4 and is subjected to the 60-percent threshold. If this frame is added to the queue, the threshold will be exceeded, so the switch drops it.

Related Topics

Configuring Queue Limits (CLI), on page 679
Examples: Queue-limit Configuration, on page 702

Weighted Tail Drop Default Values

The following are the Weighted Tail Drop (WTD) default values and the rules for configuring WTD threshold values.

- If you configure less than three queue-limit percentages for WTD, then WTD default values are assigned to these thresholds.

The following are the WTD threshold default values:

Table 40: WTD Threshold Default Values

Threshold	Default Value Percentage
0	80
1	90
2	400

- If 3 different WTD thresholds are configured, then the queues are programmed as configured.
- If 2 WTD thresholds are configured, then the maximum value percentage will be 400.
- If a WTD single threshold is configured as x, then the maximum value percentage will be 400.
  - If the value of x is less than 90, then threshold1=90 and threshold 0= x.
  - If the value of x equals 90, then threshold1=90, threshold 0=80.
  - If the value x is greater than 90, then threshold1=x, threshold 0=80.

Priority Queues

Each port supports eight egress queues, of which two can be given a priority.

You use the **priority level** policy class-map command to configure the priority for two classes. One of the classes has to be configured with a priority queue level 1, and the other class has to be configured with a priority queue level 2. Packets on these two queues are subjected to less latency with respect to other queues.

Note You can configure a priority only with a level.

Only one strict priority or a priority with levels is allowed in one policy map. Multiple priorities with the same priority levels without kbps/percent are allowed in a policy map only if all of them are configured with police.

Related Topics

Configuring Priority (CLI), on page 674

Queue Buffer

In Cisco IOS XE Release 3.7.5 E and later releases, all downlink ports are allocated 1 GB port buffer, even though the downlink port size is 10GB. Prior to this change, all 1 GB downlink ports had 1 GB buffer and 10 GB downlink ports had 10 GB buffer.

At boot time, when there is no policy map enabled on the wired port, there are two queues created by default. Wired ports can have a maximum of 8 queues configured using MQC-based policies. The following table shows which packets go into which one of the queues:

Table 41: DSCP, Precedence, and CoS - Queue Threshold Mapping Table

DSCP, Precedence or CoS	Queue	Threshold
Control Packets	0	2
Rest of Packets	1	2

Note You can guarantee the availability of buffers, set drop thresholds, and configure the maximum memory allocation for a queue. You use the **queue-buffers** policy-map class command to configure the queue buffers. You use the **queue-limit** policy-map class command to configure the maximum thresholds.

There are two types of buffer allocations: hard buffers, which are explicitly reserved for the queue, and soft buffers, which are available for other ports when unused by a given port.

For the wireless port default, Queue 0 will be given 40 percent of the buffers that are available for the interface as hard buffers, that is 67 buffers are allocated for Queue 0 in the context of 1-gigabit ports. The soft maximum for this queue is set to 268 (calculated as 67 * 400/100) for 1-gigabit ports, where 400 is the default maximum threshold that is configured for any queue.

For the wired port default, Queue 0 will be given 40 percent of the buffers that are available for the interface as hard buffers, that is 120 buffers are allocated for Queue 0 in the context of 1-gigabit ports, and 720 buffers in the context of 10-gigabit ports. The soft maximum for this queue is set to 480 (calculated as 120 * 400/100) for 1-gigabit ports and 2880 for 10-gigabit ports, where 400 is the default maximum threshold that is configured for any queue.

Queue Buffer Allocation

The buffer allocation to any queue can be tuned using the **queue-buffers ratio** policy-map class configuration command.

Related Topics

Configuring Queue Buffers (CLI), on page 677
Examples: Queue Buffers Configuration, on page 703

Dynamic Threshold and Scaling

Traditionally, reserved buffers are statically allocated for each queue. No matter whether the queue is active or not, its buffers are held up by the queue. In addition, as the number of queues increases, the portion of the reserved buffers allocated for each queue can become smaller and smaller. Eventually, a situation may occur where there are not enough reserved buffers to support a jumbo frame for all queues.

The switch supports Dynamic Thresholding and Scaling (DTS), which is a feature that provides a fair and efficient allocation of buffer resources. When congestion occurs, this DTS mechanism provides an elastic buffer allocation for the incoming data based on the occupancy of the global/port resources. Conceptually, DTS scales down the queue buffer allocation gradually as the resources are used up to leave room for other queues, and vice versa. This flexible method allows the buffers to be more efficiently and fairly utilized.

As mentioned in the previous sections, there are two limits configured on a queue—a hard limit and a soft limit.

Hard limits are not part of DTS. These buffers are available only for that queue. The sum of the hard limits should be less than the globally set up hard maximum limit. The global hard limit configured for egress

queuing is currently set to 5705. In the default scenario when there are no MQC policies configured, the 24 1-gigabit ports would take up 24 * 67 = 1608, and the 4 10-gigabit ports would take up 4 * 720 = 2880, for a total of 4488 buffers, allowing room for more hard buffers to be allocated based upon the configuration.

Soft limit buffers participate in the DTS process. Additionally, some of the soft buffer allocations can exceed the global soft limit allocation. The global soft limit allocation for egress queuing is currently set to 7607. The sum of the hard and soft limits add up to 13312, which in turn translates to 3.4 MB. Because the sum of the soft buffer allocations can exceed the global limit, it allows a specific queue to use a large number of buffers when the system is lightly loaded. The DTS process dynamically adjusts the per-queue allocation as the system becomes more heavily loaded.

Queuing in Wireless

Queuing in the wireless component is performed based on the port policy and is applicable only in the downstream direction. The wireless module supports the following four queues:

- Voice—This is a strict priority queue. Represented by Q0, this queue processes control traffic and multicast or unicast voice traffic. All control traffic (such as CAPWAP packets) is processed through the voice queue. The QoS module uses a different threshold within the voice queue to process control and voice packets to ensure that control packets get higher priority over other non-control packets.
- Video—This is a strict priority queue. Represented by Q1, this queue processes multicast or unicast video traffic.
- Data NRT—Represented by Q2, this queue processes all non-real-time unicast traffic.
- Multicast NRT—Represented by Q3, this queue processes Multicast NRT traffic. Any traffic that does not match the traffic in Q0, Q1, or Q2 is processed through Q3.

Note By default, the queues Q0 and Q1 are not enabled.

Note A weighted round-robin policy is applied for traffic in the queues Q2 and Q3.

For upstream direction only one queue is available. Port and radio policies are applicable only in the downstream direction.

Note The wired ports support eight queues.

Trust Behavior

Trust Behavior for Wired and Wireless Ports

For wired or wireless ports that are connected to the switch (end points such as IP phones, laptops, cameras, telepresence units, or other devices), their DSCP, precedence, or CoS values coming in from these end points are trusted by the switch and therefore are retained in the absence of any explicit policy configuration.

This trust behavior is applicable to both upstream and downstream QoS.

The packets are enqueued to the appropriate queue per the default initial configuration. No priority queuing at the switch is done by default. This is true for unicast and multicast packets.

In scenarios where the incoming packet type differs from the outgoing packet type, the trust behavior and the queuing behavior are explained in the following table. Note that the default trust mode for a port is DSCP based. The trust mode 'falls back' to CoS if the incoming packet is a pure Layer 2 packet. You can also change the trust setting from DSCP to CoS. This setting change is accomplished by using an MQC policy that has a class default with a 'set cos cos table default default-cos' action, where default-cos is the name of the table map created (which only performs a default copy).

Table 42: Trust and Queueing Behavior

Incoming Packet	Outgoing Packet	Trust Behavior	Queuing Behavior
Layer 3	Layer 3	Preserve DSCP/Precedence	Based on DSCP
Layer 2	Layer 2	Not applicable	Based on CoS
Tagged	Tagged	Preserve DSCP and CoS	Based on DSCP (trust DSCP takes precedence)
Layer 3	Tagged	Preserve DSCP, CoS is set to 0	Based on DSCP

The Cisco IOS XE 3.2 Release supported different trust defaults for wired and wireless ports. The trust default for wired ports was the same as for this software release. For wireless ports, the default system behavior was non-trust, which meant that when the switch came up, all markings for the wireless ports were defaulted to zero and no traffic received priority treatment. For compatibility with an existing wired switch, all traffic went to the best-effort queue by default. The access point performed priority queuing by default. In the downstream direction, the access point maintained voice, video, best-effort, and background queues for queuing. The access selected the queuing strategy based on the 11e tag information. By default, the access point treated all wireless packets as best effort.

Related Topics

Configuring Trust Behavior for Wireless Traffic (CLI), on page 663
Example: Table Map Configuration to Retain CoS Markings, on page 707

Port Security on a Trusted Boundary for Cisco IP Phones

In a typical network, you connect a Cisco IP Phone to a switch port and cascade devices that generate data packets from the back of the telephone. The Cisco IP Phone guarantees the voice quality through a shared data link by marking the CoS level of the voice packets as high priority (CoS = 5) and by marking the data packets as low priority (CoS = 0). Traffic sent from the telephone to the switch is typically marked with a tag that uses the 802.1Q header. The header contains the VLAN information and the class of service (CoS) 3-bit field, which is the priority of the packet.

For most Cisco IP Phone configurations, the traffic sent from the telephone to the switch should be trusted to ensure that voice traffic is properly prioritized over other types of traffic in the network. By using the **trust device** interface configuration command, you configure the switch port to which the telephone is connected to trust the traffic received on that port.

Note The **trust device** *device_type* command available in interface configuration mode is a stand-alone command on the switch. When using this command in an AutoQoS configuration, if the connected peer device is not a corresponding device (defined as a device matching your trust policy), both CoS and DSCP values are set to "0" and any input policy will not take effect. If the connected peer device is a corresponding device, input policy will take effect.

With the trusted setting, you also can use the trusted boundary feature to prevent misuse of a high-priority queue if a user bypasses the telephone and connects the PC directly to the switch. Without trusted boundary, the CoS labels generated by the PC are trusted by the switch (because of the trusted CoS setting). By contrast, trusted boundary uses CDP to detect the presence of a Cisco IP Phone (such as the Cisco IP Phone 7910, 7935, 7940, and 7960) on a switch port. If the telephone is not detected, the trusted boundary feature disables the trusted setting on the switch port and prevents misuse of a high-priority queue. Note that the trusted boundary feature is not effective if the PC and Cisco IP Phone are connected to a hub that is connected to the switch.

Wireless QoS Mobility

Wireless QoS mobility enables you to configure QoS policies so that the network provides the same service anywhere in the network. A wireless client can roam from one location to another and as a result the client can get associated to different access points associated with a different switch. Wireless client roaming can be classified into two types:

- Intra-switch roaming
- Inter-switch roaming

Note The client policies must be available on all of the switches in the mobility group. The same SSID and port policy must be applied to all switches in the mobility group so that the clients get consistent treatment.

Inter-Switch Roaming

When a client roams from one location to another, the client can get associated to access points either associated to the same switch (anchor switch) or a different switch (foreign switch). Inter-switch roaming refers to the scenario where the client gets associated to an access point that is not associated to the same device before the client roamed. The host device is now foreign to the device to which the client was initially anchored.

In the case of inter-switch roaming, the client QoS policy is always executed on the foreign controller. When a client roams from anchor switch to foreign switch, the QoS policy is uninstalled on the anchor switch and installed on the foreign switch. In the mobility handoff message, the anchor device passes the name of the policy to the foreign switch. The foreign switch should have a policy with the same name configured for the QoS policy to be applied correctly.

In the case of inter-switch roaming, all of the QoS policies are moved from the anchor device to the foreign device. While the QoS policies are in transition from the anchor device to the foreign device, the traffic on the foreign device is provided the default treatment. This is comparable to a new policy installation on the client target.

Note If the foreign device is not configured with the user-defined physical port policy, the default port policy is applicable to all traffic is routed through the NRT queue, except the control traffic which goes through RT1 queue. The network administrator must configure the same physical port policy on both the anchor and foreign devices symmetrically.

During inter-switch roaming, client and SSID policy statistics are collected only for the duration that the client is associated with the foreign switch. Cumulative statistics for the whole roaming (anchor switch and foreign switch) are not collected.

Intra-Switch Roaming

With intra-switch roaming, the client gets associated to an access point that is associated to the same switch before the client roamed, but this association to the device occurs through a different access point.

Note QoS policies remain intact in the case of intra-switch roaming.

Precious Metal Policies for Wireless QoS

Wireless QoS is backward compatible with the precious metal policies offered by the unified wireless controller platforms. The precious metal policies are system-defined policies that are available on the controller.

The following policies are available:

- Platinum—Used for VoIP clients.
- Gold—Used for video clients.
- Silver— Used for traffic that can be considered best-effort.
- Bronze—Used for NRT traffic.

These policies (also known as profiles) can be applied to a WLAN based on the traffic. We recommend the configuration using the Cisco IOS MQC configuration. The policies are available in the system based on the precious metal policy required. You can configure precious metal policies only for SSID ingress and egress policies.

Based on the policies applied, the 802.1p, 802.11e (WMM), and DSCP fields in the packets are affected. These values are preconfigured and installed when the switch is booted.

Note Unlike the precious metal policies that were applicable in the Cisco Unified Wireless controllers, the attributes rt-average-rate, nrt-average-rate, and peak rates are not applicable for the precious metal policies configured on this switch platform.

Note The 802.1p protocol priority is applicable on the Cisco 5700 Series Wireless Controller.

Related Topics

Configuring Precious Metal Policies (CLI), on page 683

Standard QoS Default Settings

Default Wired QoS Configuration

There are two queues configured by default on each wired interface on the switch. All control traffic traverses and is processed through queue 0. All other traffic traverses and is processed through queue 1.

DSCP Maps

Default CoS-to-DSCP Map

When DSCP transparency mode is disabled, the DSCP values are derived from CoS as per the following table. If these values are not appropriate for your network, you need to modify them.

Note The DSCP transparency mode is disabled by default. If it is enabled (**no mls qos rewrite ip dscp** interface configuration command), DSCP rewrite will not happen.

Table 43: Default CoS-to-DSCP Map

CoS Value	DSCP Value
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

Default IP-Precedence-to-DSCP Map

You use the IP-precedence-to-DSCP map to map IP precedence values in incoming packets to a DSCP value that QoS uses internally to represent the priority of the traffic. The following table shows the default IP-precedence-to-DSCP map. If these values are not appropriate for your network, you need to modify them.

Table 44: Default IP-Precedence-to-DSCP Map

IP Precedence Value	DSCP Value
0	0
1	8

IP Precedence Value	DSCP Value
2	16
3	24
4	32
5	40
6	48
7	56

Default DSCP-to-CoS Map

You use the DSCP-to-CoS map to generate a CoS value, which is used to select one of the four egress queues. The following table shows the default DSCP-to-CoS map. If these values are not appropriate for your network, you need to modify them.

Table 45: Default DSCP-to-CoS Map

DSCP Value	CoS Value
0–7	0
8–15	1
16–23	2
24–31	3
32–39	4
40–47	5
48–55	6
56–63	7

Default Wireless QoS Configuration

The ports on the switch do not distinguish between wired or wireless physical ports. Depending on the kind of device associated to the switch, the policies are applied. For example, when an access point is connected to a switch port, the switch detects it as a wireless device and applies the default hierarchical policy which is in the format of a parent-child policy. This policy is an hierarchical policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suite the QoS configuration. The switch is preconfigured with a default class map and a policy map.

Configuring Auto QoS for Wireless

Information About Auto QoS for Wireless

Auto QoS for Wireless feature, introduced in Cisco IOS XE Release 3.7.0, is supported on the following platforms:

- Cisco 5760 Wireless Controller
- Catalyst 3850 Series Switches
- Catalyst 3650 Series Switches
- Cisco Catalyst 4500E Supervisor Engine 8-E

The following pre-defined global configuration templates/profiles are available:

- Enterprise
- Voice
- Guest

You can customize these templates to suit your needs. Auto QoS for Wireless can be configured using both CLI and GUI. Auto QoS for Wireless can be applied on a per-WLAN basis.

Precedence applicable:

1. AAA QoS
2. Native Profile QoS
3. Auto QoS/CLI-based QoS

Policy Names

P1	AutoQos-4.0-wlan-ET-Client-Input-Policy
P2	AutoQos-4.0-wlan-ET-SSID-Output-Policy
P3	platinum-up (Auto generated system policy at boot-up)
P4	platinum (Auto generated system policy at boot-up)
P5	AutoQos-4.0-wlan-GT-SSID-Input-Policy
P6	AutoQos-4.0-wlan-GT-SSID-Output-Policy
P7	port_child_policy
P8	AutoQos-4.0-wlan-Port-Output-Policy
P9	Capwap-SRND4-Queuing-Policy

List of Targets

- Client
- BSSID
- Radio
- AP Port (Catalyst 3850 Switch)
- Uplink Port (Catalyst 3850 Switch)
- Cisco 5760 WLC physical port
- Catalyst 4500E Supervisor Engine 8-E Front Panel Ports

Auto QoS for Wireless - Wireless QoS Matrix

Templates	Client		BSSID		Radio	AP Port (Catalyst 3850 Switch)		Uplink Port (Catalyst 3850 Switch)		Cisco 5760 WLC physical port		Catalyst 4500E Supervisor Engine 8-E Front Panel Ports	
	Ingress	Egress	Ingress	Egress		Ingress	Egress	Ingress	Egress	Ingress	Egress	Ingress	Egress
Enterprise	P1	N/A	N/A	P2	N/A	N/A	P7	N/A	N/A	N/A	P8	N/A	P9
Voice	N/A	N/A	P3	P4	N/A	N/A	P7	N/A	N/A	N/A	P8	N/A	P9
Guest	N/A	N/A	P5	P6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	P9

Guidelines for Auto QoS for Wireless

- The Catalyst 3850 Switch uplink ports should not be configured along with Auto QoS for Wireless. This should be managed using Wired Auto QoS
- The Catalyst 3850 Switch AP Port Policy (port_child_policy) and Cisco 5760 WLC physical ports should be automatically configured for Enterprise and Voice templates.
- AP Control traffic must go through the P0 queue (should be given highest priority among all traffic).
- All the Auto QoS policies for Wireless applied through the GUI have the prefix 'AutoQos-4.0'. This enables you to recognize the policies that are applied through templates.
- On the CLI, it is not possible to create a policy name that starts with 'AutoQos-4.0' because this is reserved for policies generated through templates.

Configuring Auto QoS for Wireless (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **WLAN**.

Step 2 Click the WLAN ID.

Step 3 Click the QoS tab.

Step 4 In the **Auto QoS** section, choose the policy from the drop-down list.

Note By default, the Auto QoS policy applied for a WLAN is 'None'.

Step 5 Save the configuration.

Configuring Auto QoS for Wireless (CLI)

```
Switch(config-wlan)# auto qos {enterprise | guest | voice}
```

Guidelines for QoS Policies

Follow these guidelines to prevent clients from getting excluded due to malformed QoS policies:

- When a new QoS policy is added to the switch, a QoS policy with the same name should be added to other switch within the same roam or mobility domain.
- When a switch is loaded with a software image of a later release, the new policy formats are supported. If you have upgraded the software image from an earlier release to a later release, you should save the configuration separately. When an earlier release image is loaded, some QoS policies might show as not supported, and you should restore those QoS policies to supported policy formats.

Restrictions for QoS on Wired Targets

A target is an entity where a policy is applied. You can apply a policy to either a wired or wireless target. A wired target can be either a port or VLAN. A wireless target can be either a port, radio, SSID, or client. Only port, SSID, and client policies are user configurable. Radio polices are not user configurable. Wireless QoS policies for port, radio, SSID, and client are applied in the downstream direction, and for upstream only SSID and client targets are supported. Downstream indicates that traffic is flowing from the switch to the wireless client. Upstream indicates that traffic is flowing from wireless client to the switch.

The following are restrictions for applying QoS features on the switch for the wired target:

- A maximum of 8 queuing classes are supported on the switch port for the wired target.
- A maximum of 63 policers are supported per policy on the wired port for the wired target.
- In Cisco IOS XE Release 3.7.5E and later releases, by default all downlink ports are allocated 1 GB port buffer, even though the downlink port size is 10 GB. Prior to this change, all 1 GB downlink ports had 1 GB buffer and 10 GB downlink ports had 10 GB buffer.
- A maximum of 1599 policy-maps can be created.
- No more than two levels are supported in a QoS hierarchy.
- In a hierarchical policy, overlapping actions between parent and child are not allowed, except when a policy has the port shaper in the parent and queueing features in the child policy.
- A QoS policy cannot be attached to any EtherChannel interface.

- Policing in both the parent and child is not supported in a QoS hierarchy.
- Marking in both the parent and child is not supported in a QoS hierarchy.
- A mixture of queue limit and queue buffer in the same policy is not supported.

Note The queue-limit percent is not supported on the switch because the **queue-buffer** command handles this functionality. Queue limit is only supported with the DSCP and CoS extensions.

- With shaping, there is an IPG overhead of 20Bytes for every packet that is accounted internally in the hardware. Shaping accuracy will be effected by this, specially for packets of small size.
- The classification sequence for all wired queuing-based policies should be the same across all wired upstream ports (10-Gigabit Ethernet), and the same for all downstream wired ports (1-Gigabit Ethernet).
- Empty classes are not supported.
- Class-maps with empty actions are not supported. If there are two policies with the same order of class-maps and if there are class-maps with no action in one of the policies, there may be traffic drops. As a workaround, allocate minimal bandwidth for all the classes in PRIORITY_QUEUE.
- A maximum of 256 classes are supported per policy on the wired port for the wired target.
- The actions under a policer within a policy map have the following restrictions:
  - The conform action must be transmit.
  - The exceed/violate action for markdown type can only be cos2cos, prec2prec, dscp2dscp.
  - The markdown types must be the same within a policy.
- A port-level input marking policy takes precedence over an SVI policy; however, if no port policy is configured, the SVI policy takes precedence. For a port policy to take precedence, define a port-level policy; so that the SVI policy is overwritten.
- Classification counters have the following specific restrictions:
  - Classification counters count packets instead of bytes.
  - Filter-based classification counters are not supported
  - Only QoS configurations with marking or policing trigger the classification counter.
  - The classification counter is not port based. This means that the classification counter aggregates all packets belonging to the same class of the same policy which attach to different interfaces.
  - As long as there is policing or marking action in the policy, the class-default will have classification counters.
  - When there are multiple match statements in a class, then the classification counter only shows the traffic counter for one of the match statements.
- Table maps have the following specific restrictions:
  - Only one table map for policing exceeding the markdown and one table map for policing violating the markdown per direction per target is supported.

- Table maps must be configured under the class-default; table maps are unsupported for a user-defined class.

- Hierarchical policies are required for the following:
  - Port-shapers
  - Aggregate policers
  - PV policy
  - Parent shaping and child marking/policing
- In a HQoS policy with parent shaping and child policy having priority level queuing and priority level policing, the statistics for policing are not updated. Only QoS shaper statistics are updated. To view the QoS shaper statistics, use the **show policy-map interface** command in global configuration mode.
- For ports with wired targets, these are the only supported hierarchical policies:
  - Police chaining in the same policy is unsupported, except for wireless client.
  - Hierarchical queueing is unsupported in the same policy (port shaper is the exception).
  - In a parent class, all filters must have the same type. The child filter type must match the parent filter type with the following exceptions:
    - If the parent class is configured to match IP, then the child class can be configured to match the ACL.
    - If the parent class is configured to match CoS, then the child class can be configured to match the ACL.
- The **trust device** *device_type* command available in interface configuration mode is a stand-alone command on the switch. When using this command in an AutoQoS configuration, if the connected peer device is not a corresponding device (defined as a device matching your trust policy), both CoS and DSCP values are set to "0" and any input policy will not take effect. If the connected peer device is a corresponding device, input policy will take effect.

The following are restrictions for applying QoS features on the VLAN to the wired target:

- For a flat or nonhierarchical policy, only marking or a table map is supported.

The following are restrictions and considerations for applying QoS features on EtherChannel and channel member interfaces:

- QoS is not supported on an EtherChannel interface.
- QoS is supported on EtherChannel member interfaces in both ingress and egression directions. All EtherChannel members must have the same QoS policy applied. If the QoS policy is not the same, each individual policy on the different link acts independently.
- On attaching a service policy to channel members, the following warning message appears to remind the user to make sure the same policy is attached to all ports in the EtherChannel: ' Warning: add service policy will cause inconsistency with port xxx in ether channel xxx. '.
- Auto QoS is not supported on EtherChannel members.

Note On attaching a service policy to an EtherChannel, the following message appears on the console: ' Warning: add service policy will cause inconsistency with port xxx in ether channel xxx. '. This warning message should be expected. This warning message is a reminder to attach the same policy to other ports in the same EtherChannel. The same message will be seen during boot up. This message does not mean there is a discrepancy between the EtherChannel member ports.

Related Topics

Restrictions for QoS on Wireless Targets, on page 632
Prerequisites for Quality of Service, on page 589
QoS Overview, on page 591
QoS Implementation, on page 602

Restrictions for QoS on Wireless Targets

General Restrictions

A target is an entity where a policy is applied. You can apply a policy to either a wired or wireless target. A wired target can be either a port or VLAN. A wireless target can be either a port, radio, SSID, or client. Only port, SSID, and client policies are user configurable. Radio polices are not user configurable. Wireless QoS policies for port, radio, SSID, and client are applied in the downstream direction, and for upstream only SSID and client targets are supported. Downstream indicates that traffic is flowing from the switch to the wireless client. Upstream indicates that traffic is flowing from wireless client to the switch.

- Only port, SSID, and client (using AAA and Cisco IOS command-line interface) policies are user-configurable. Radio policies are set by the wireless control module and are not user-configurable.
- Port and radio policies are applicable only in the egress direction.
- SSID and client targets can be configured only with marking and policing policies.
- One policy per target per direction is supported.
- For the egress class-default SSID policy, you must configure the queue buffer ratio as 0 after you configure the average shape rate.
- Class maps in a policy map can have different types of filters. However, only one marking action (either table map, or set dscp, or set cos) is supported in a map in egress direction.
- For hierarchical client and SSID ingress policies, you cannot configure marking in both the parent and child policies. You can only configure marking either in the parent or child policy.
- You cannot configure multiple set actions in the same class.
- For both SSID and client ingress policies, supported set actions are only for DSCP, and CoS values.
- You cannot delete a group of WLANs or QoS policy.

Wireless QoS Restrictions on Ports

The following are restrictions for applying QoS features on a wireless port target:

- All wireless ports have similar parent policy with one class-default and one action shape under class-default. Shape rates are dependent on the 802.11a/b/g/ac bands.

- You can create a maximum of four classes in a child policy by modifying the `port_chlid_policy`.
- If there are four classes in the `port_child_policy` at the port level, one must be a non-client-nrt class and one must be class-default.
- No two classes can have the same priority level. Only priority level 1 (for voice traffic and control traffic) and 2 (for video) are supported.
- Priority is not supported in the multicast NRT class (non-client-nrt class) and `class-default`.
- If four classes are configured, two of them have to be priority classes. If only three classes are configured, at least one of them should be a priority class. If three classes are configured and there is no non-client-nrt class, both priority levels must be present.
- Only match DSCP is supported.
- The port policy applied by the wireless control module cannot be removed using the CLI.
- Both priority rate and police CIR (using MQC) in the same class is unsupported.
- Queue limit (which is used to configure Weighted Tail Drop) is unsupported.

Wireless QoS Restrictions on SSID

The following are restrictions for applying QoS features on SSID:

- One table map is supported at the ingress policy.
- Table maps are supported for the parent class-default only. Up to two table maps are supported in the egress direction and three table-maps can be configured when a QoS group is involved.

Note Table-maps are not supported at the client targets.

- If a wireless port has a default policy with only two queues (one for multicast-NRT, one for class-default), the policy at SSID level cannot have voice and video class in the egress direction.
- Policing without priority is not supported in the egress direction.
- Priority configuration at the SSID level is used only to configure the RT1 and RT2 policers (AFD for policer). Priority configuration does not include the shape rate. Therefore, priority is restricted for SSID policies without police.
- If **set** is not enabled in class-default, the classification at the SSID for voice or video must be a subset of the classification for the voice or video class at the port level.
- The mapping in the DSCP2DSCP and COS2COS table should be based on the classification function for the voice and video classes in the port level policy.
- No action is allowed under the class-default of a child policy.
- For SSID ingress policies, only UP and DSCP filters (match criteria) are supported. ACL and protocol match criteria are not supported.
- For a flat policy (non hierarchical), in the ingress direction, the policy configuration must be a set (table map) or policing or both.

Wireless QoS Restrictions on Clients

The following are restrictions for applying QoS policies on client targets:

- The default client policy is enabled only on WMM clients that are ACM-enabled.
- Queuing is not supported.
- Attaching, removing, or modifying client policies on a WLAN in the enabled state is not supported. You must shut down the WLAN to apply, remove, or modify a policy.
- Table-map configuration is not supported for client targets.
- Policing and set configured together in class-default is blocked in egress direction:

```
policy-map foo
class class-default
police X
set dscp Y
```

- Child policy is not supported under class-default if the parent policy contains other user-defined class maps in it.
- For flat egress client policy, policing in class-default and marking action in other classes are not supported.
- Only set marking actions are supported in the client policies.
- For client ingress policies, only ACL, UP, DSCP, and protocol filters (match criteria) are supported.
- All the filters in classes in a policy map for client policy must have the same attributes. Filters matching on protocol-specific attributes such as IPv4 or IPv6 addresses are considered as different attribute sets.
- For filters matching on ACLs, all ACEs (Access Control Entry) in the access list should have the same type and number of attributes.
- In client egress policies, all filters in the policy-map must match on the same marking attribute for filters matching on marking attributes. For example, If filter matches on DSCP, then all filters in the policy must match on DSCP.
- ACL matching on port ranges and subnet are only supported in ingress direction.

Related Topics

Configuring Port Policies (GUI), on page 685
Applying or Changing Port Policies (GUI), on page 686
Applying a QoS Policy on a WLAN (GUI), on page 687
Port Policies, on page 596
Port Policy Format, on page 596
Radio Policies, on page 598
Restrictions for QoS on Wired Targets, on page 629
Prerequisites for Quality of Service, on page 589
QoS Overview, on page 591
QoS Implementation, on page 602

How to Configure QoS

Configuring Class, Policy, and Table Maps

Creating a Traffic Class (CLI)

To create a traffic class containing match criteria, use the **class-map** command to specify the traffic class name, and then use the following **match** commands in class-map configuration mode, as needed.

Before you begin

All match commands specified in this configuration task are considered optional, but you must configure at least one match criterion for a class.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

Step 2	**class-map** *class-map name* { **match-any** | **match-all** }
	Example:
	`Switch(config)# class-map test_1000`
	`Switch(config-cmap)#`
		Enters class map configuration mode.
		• Creates a class map to be used for matching packets to the class whose name you specify.
		• **match-any:** Any one of the match criteria must be met for traffic entering the traffic class to be classified as part of it.
		• **match-all:** All of the match criteria must be met for traffic entering the traffic class to be classified as part of the traffic class.
		Note This is the default. If **match-any** or **match-all** is not explicitly defined, **match-all** is chosen by default.

Step 3	**match access-group** {*index number* | *name*}
	Example:
	`Switch(config-cmap)# match access-group 100`
	`Switch(config-cmap)#`
		The following parameters are available for this command:
		• access-group
		• class-map
		• cos

	Command or Action	Purpose
		• dscp • ip • non-client-nrt • precedence • qos-group • vlan • wlan user priority (Optional) For this example, enter the access-group ID: • Access list index (value from 1 to 2799) • Named access list

Step 4	**match class-map** *class-map name*
	Example:
	`Switch(config-cmap)# match class-map test_2000`
	`Switch(config-cmap)#`
		(Optional) Matches to another class-map name.

Step 5	**match cos** *cos value*
	Example:
	`Switch(config-cmap)# match cos 2 3 4 5`
	`Switch(config-cmap)#`
		(Optional) Matches IEEE 802.1Q or ISL class of service (user) priority values.
		• Enters up to 4 CoS values separated by spaces (0 to 7).

Step 6	**match dscp** *dscp value*
	Example:
	`Switch(config-cmap)# match dscp af11 af12`
	`Switch(config-cmap)#`
		(Optional) Matches the DSCP values in IPv4 and IPv6 packets.

Step 7	**match ip** {**dscp** *dscp value* | **precedence** *precedence value* }
	Example:
	`Switch(config-cmap)# match ip dscp af11 af12`
	`Switch(config-cmap)#`
		(Optional) Matches IP values including the following:
		• **dscp**—Matches IP DSCP (DiffServ codepoints).
		• **precedence**—Matches IP precedence (0 to 7).

	Command or Action	Purpose
		Note Since CPU generated packets are not marked at egress, the packet will not match the configured class-map.

Step 8	**match non-client-nrt**
	Example:
	`Switch(config-cmap)# match non-client-nrt`
	`Switch(config-cmap)#`
		(Optional) Matches non-client NRT (Non-Real-Time).
		Note This match is applicable only for policies on a wireless port. It carries all the multi-destination and AP (non-client) bound traffic.

Step 9	**match qos-group** *qos group value*
	Example:
	`Switch(config-cmap)# match qos-group 10`
	`Switch(config-cmap)#`
		(Optional) Matches QoS group value (from 0 to 31).

Step 10	**match vlan** *vlan value*
	Example:
	`Switch(config-cmap)# match vlan 210`
	`Switch(config-cmap)#`
		(Optional) Matches a VLAN ID (from 1 to 4095).

Step 11	**match wlan user-priority** *wlan value*
	Example:
	`Switch(config-cmap)# match wlan user priority 7`
	`Switch(config-cmap)#`
		(Optional) Matches 802.11e specific values. Enter the user priority 802.11e user priority (0 to 7).

Step 12	**end** **Example:** `Switch(config-cmap)# end`	Saves the configuration changes.

What to do next

Configure the policy map.

Related Topics

Class Maps, on page 608
Examples: Classification by Access Control Lists, on page 692

Creating a Traffic Policy (CLI)

To create a traffic policy, use the **policy-map** global configuration command to specify the traffic policy name.

The traffic class is associated with the traffic policy when the **class** command is used. The **class** command must be entered after you enter the policy map configuration mode. After entering the **class** command, the switch is automatically in policy map class configuration mode, which is where the QoS policies for the traffic policy are defined.

The following policy map class-actions are supported:

- admit—Admits the request for Call Admission Control (CAC).
- bandwidth—Bandwidth configuration options.
- exit—Exits from the QoS class action configuration mode.
- no—Negates or sets default values for the command.
- police—Policer configuration options.
- priority—Strict scheduling priority configuration options for this class.
- queue-buffers—Queue buffer configuration options.
- queue-limit—Queue maximum threshold for Weighted Tail Drop (WTD) configuration options.
- service-policy—Configures the QoS service policy.
- set—Sets QoS values using the following options:
  - CoS values
  - DSCP values
  - Precedence values
  - QoS group values
  - WLAN values
- shape—Traffic-shaping configuration options.

Before you begin

You should have first created a class map.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose

Step 2	**policy-map** *policy-map name*
	Example:
	`Switch(config)# policy-map test_2000`
	`Switch(config-pmap)#`
		Enters policy map configuration mode.
		Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

Step 3	**class** {*class-name* | **class-default**}
	Example:
	`Switch(config-pmap)# class test_1000`
	`Switch(config-pmap-c)#`
		Specifies the name of the class whose policy you want to create or change.
		You can also create a system default class for unclassified packets.

Step 4	**admit**
	Example:
	`Switch(config-pmap-c)# admit cac wmm-tspec`
	`Switch(config-pmap-c)#`
		(Optional) Admits the request for Call Admission Control (CAC). For a more detailed example of this command and its usage, see the section Configuring Call Admission Control.
		Note This command only configures CAC for wireless QoS.

Step 5	**bandwidth** {**kb/s** *kb/s value* | **percent** *percentage* | **remaining** {*percent* | *ratio*}}
	Example:
	`Switch(config-pmap-c)# bandwidth 50`
	`Switch(config-pmap-c)#`
		(Optional) Sets the bandwidth using one of the following:
		• **kb/s**—Kilobits per second, enter a value between 20000 and 10000000 for Kb/s.
		• **percent**—Enter the percentage of the total bandwidth to be used for this policy map.
		• **remaining**—Enter the percentage ratio of the remaining bandwidth.
		For a more detailed example of this command and its usage, see Configuring Bandwidth (CLI), on page 670.

Step 6	**exit**
	Example:
	`Switch(config-pmap-c)# exit`
	`Switch(config-pmap-c)#`
		(Optional) Exits from QoS class action configuration mode.

Step 7	**no** **Example:** `Switch(config-pmap-c)# no`	(Optional) Negates the command.

	Command or Action	Purpose
	`Switch(config-pmap-c)#`	

Step 8	**police** {*target_bit_rate* | **cir** | **rate**}
	Example:
	`Switch(config-pmap-c)# police 100000`
	`Switch(config-pmap-c)#`
		(Optional) Configures the policer:
		• *target_bit_rate*—Enter the bit rate per second, enter a value between 8000 and 10000000000.
		• **cir**—Committed Information Rate
		• **rate**—Specify police rate, PCR for hierarchical policies or SCR for single-level ATM 4.0 policer policies.
		For a more detailed example of this command and its usage, see Configuring Police (CLI), on page 672.

Step 9	**priority** {*kb/s* | **level** *level value* | **percent** *percentage value*}
	Example:
	`Switch(config-pmap-c)# priority percent 50`
	`Switch(config-pmap-c)#`
		(Optional) Sets the strict scheduling priority for this class. Command options include:
		• *kb/s*—Kilobits per second, enter a value between 1 and 2000000.
		• **level**—Establishes a multi-level priority queue. Enter a value (1 or 2).
		• **percent**—Enter a percent of the total bandwidth for this priority.
		For a more detailed example of this command and its usage, see Configuring Priority (CLI), on page 674.

Step 10	**queue-buffers ratio** *ratio limit*
	Example:
	`Switch(config-pmap-c)# queue-buffers ratio 10`
	`Switch(config-pmap-c)#`
		(Optional) Configures the queue buffer for the class. Enter the queue buffers ratio limit (0 to 100).
		For a more detailed example of this command and its usage, see Configuring Queue Buffers (CLI), on page 677.

Step 11	**queue-limit** {*packets* | **cos** | **dscp** | **percent**}
	Example:
	`Switch(config-pmap-c)# queue-limit cos 7 percent 50`
	`Switch(config-pmap-c)#`
		(Optional) Specifies the queue maximum threshold for the tail drop:
		• *packets*—Packets by default, enter a value between 1 to 2000000.
		• **cos**—Enter the parameters for each COS value.
		• **dscp**—Enter the parameters for each DSCP value.

	Command or Action	Purpose
		• **percent**—Enter the percentage for the threshold. For a more detailed example of this command and its usage, see Configuring Queue Limits (CLI), on page 679.

Step 12	**service-policy** *policy-map name*
	
	Example:
	
	`Switch(config-pmap-c)# service-policy test_2000`
	`Switch(config-pmap-c)#`
		(Optional) Configures the QoS service policy.

Step 13	**set** {**cos** | **dscp** | **ip** | **precedence** | **qos-group** | **wlan**}
	
	Example:
	
	`Switch(config-pmap-c)# set cos 7`
	`Switch(config-pmap-c)#`
		(Optional) Sets the QoS values. Possible QoS configuration values include:
		• **cos**—Sets the IEEE 802.1Q/ISL class of service/user priority.
		• **dscp**—Sets DSCP in IP(v4) and IPv6 packets.
		• **ip**—Sets IP specific values.
		• **precedence**—Sets precedence in IP(v4) and IPv6 packet.
		• **qos-group**—Sets the QoS Group.
		• **wlan**—Sets the WLAN user-priority.

Step 14	**shape average** {*target _bit_rate* | **percent**}
	
	Example:
	
	`Switch(config-pmap-c) #shape average percent 50`
	`Switch(config-pmap-c) #`
		(Optional) Sets the traffic shaping. Command parameters include:
		• *target_bit_rate*—Target bit rate.
		• **percent**—Percentage of interface bandwidth for Committed Information Rate.
		
		For a more detailed example of this command and its usage, see Configuring Shaping (CLI), on page 682.

Step 15	**end**
	
	Example:
	
	`Switch(config-pmap-c) #end`
	`Switch(config-pmap-c) #`
		Saves the configuration changes.

What to do next

Configure the interface.

Related Topics

Policy Maps, on page 608

Configuring Client Policies (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless**.

Step 2 Expand the **QoS** node by clicking on the left pane and choose **QOS-Policy**.

The **QOS-Policy** page is displayed.

Step 3 Click **Add New** to create a new QoS Policy.

The **Create QoS Policy** page is displayed.

Step 4 Select **Client** from the **Policy Type** drop-down menu.

Step 5 Select the direction into which the policy needs to be applied from the **Policy Direction** drop-down menu.

The available options are:

- **Ingress**
- **Egress**

Step 6 Specify a policy name in the **Policy Name** text box.

Step 7 Provide a description to the policy in the **Description** text box.

Step 8 (Optional) Configure the default voice or video configuration parameters by checking the **Enable Voice** or **Enable Video** checkbox.

The following options are available:

- **Trust**—Specify the classification type behavior on this policy. The options available are:
  - **DSCP**—Assigns a label to indicate the given quality of service. The range is from 0 to 63.
  - **User Priority**—This option is available when the **Policy Direction** is ingress. Enter the 802.11e user priority. The range is from 0 to 7.
  - **COS**—This option is available when the **Policy Direction** is egress. Matches IEEE 802.1Q class of service. The range is from 0 to 7.
- **Mark**—Specify the marking label for each packet. The following options are available:
  - **DSCP**—Assigns a label to indicate the given quality of service. The range is from 0 to 63.
  - **CoS**—Matches IEEE 802.1Q class of service. The range is from 0 to 7.
  - **User Priority**—Enter the 802.11e user priority. The range is from 0 to 7.
- **Police(kbps)**—Specify the policing rate in kbps.

Note The marking and policing options are optional.

Step 9 Specify the **Class-default** parameters.

The following options are available:

- **Mark**—Specify the marking label for each packet. The following options are available:
  - **DSCP**—Assigns a label to indicate the given quality of service. The range is from 0 to 63.
  - **CoS**—Matches IEEE 802.1Q class of service. The range is from 0 to 7.
  - **User Priority**—Enter the 802.11e user priority. The range is from 0 to 7.
- **Police (kbps)**—This option is available when the **Policy Direction** is egress. This option Specify the policing rate in kbps.

Note You can choose either Mark or Police action for the class-default class when creating an egress client policy.

Step 10 (Optional) To configure the AVC class map for a client policy, check the **Enable Application Recognition** check box

Note For an egress client policy, when you enable Application Recognition, the Voice, Video, and User Defined check boxes are disabled.

The following options are available:

- **Trust**—Specify a classification type for this policy.
  - **Protocol**—Allows you to choose the protocols and configure the marking and policing of the packets.
  - **Category**—Allows you to choose the category of the application. For example, browsing.
  - **Subcategory**—Allows you to choose the subcategory of the application. For example, file-sharing.
  - **Application-Group**—Allows you to choose the application group. For example, ftp-group.
- **Protocol Choice**—Choose the protocols, category, subcategory, or application group from the **Available Protocols** list into the **Assigned Protocols** to apply the marking and policing of the packets.
- **Mark**—Specify the marking label for each packet. The following options are available:
  - **DSCP**—Assigns a label to indicate the given quality of service. The range is from 0 to 63.
  - **CoS**—Matches IEEE 802.1Q class of service. The range is from 0 to 7.
  - **None**—Choose this option when you do not want to mark the packets.
- **Police (kbps)**—Specifies the policing rate in kbps. This option is available when the **Policy Direction** is egress.
- **Drop**—Drops the ingress packets that correspond to the chosen protocols.

Step 11 (Optional) To configure user defined classes, check the **User Defined Classes** checkbox.

The following options are available:

- **Trust**—Specify the classification type behavior on this policy.
  - **DSCP**—Assigns a label to indicate the given quality of service. The range is from 0 to 63.
  - **User Priority**—This option is available when the **Policy Direction** is ingress. Enter the 802.11e user priority. The range is from 0 to 7.
  - **COS**—This option is available when the **Policy Direction** is egress. Matches IEEE 802.1Q class of service. The range is from 0 to 7.
- **Mark**—Specify the marking label for each packet. The following options are available:
  - **DSCP**—Assigns a label to indicate the given quality of service. The range is from 0 to 63.
  - **CoS**—Matches IEEE 802.1Q class of service. The range is from 0 to 7.

- **User Priority**—Enter the 802.11e user priority. The range is from 0 to 7.

- **Police (kbps)**—This option is available when the **Policy Direction** is egress. This option specifies the policing rate in kbps.

Note You can add a maximum of five user-defined classes for each client policy.

Step 12 Click **Add** to add the policy.

Related Topics

Client Policies, on page 599
Supported QoS Features on Wireless Targets, on page 594
Examples: Client Policies, on page 699

Configuring Client Policies

You can configure client policies using one of the following methods:

Method	Topic/Details
Default client policies	The wireless control module of the switch applies the default client policies when admission control (ACM) is enabled for WMM clients. When ACM is disabled, there is no default client policy. The default policies are: • Ingress—cldeffromWMM • Egress—cldeftoWMM You can verify if ACM is enabled by using the **show ap dot11** {**5ghz** | **24ghz**} command. To enable ACM, use the **ap dot11** {**5ghz** | **24ghz**} **cac voice acm** command.
Apply the client policy on the WLAN using the GUI.	Configuring Client Policies (GUI)
Apply the client policy on the WLAN using the CLI.	Applying an SSID or Client Policy on a WLAN (CLI)
Apply the QoS attributes policy using a local profiling policy using the CLI.	Applying a Local Policy for a Device on a WLAN (CLI)
Apply the QoS attributes policy using a local profiling policy using the GUI.	• Choose **Configuration > Security > Local Policies** to create a local profiling policy. • Choose **Configuration > Wireless > WLAN > Policy Mapping** to apply a local profiling policy on a WLAN. For more information, see Applying Local Policies to WLAN (GUI), on page 496
Apply policy map through a AAA server (ACS/ISE)	*Cisco Identity Services Engine User Guide* *Cisco Secure Access Control System User Guide*

Configuring Class-Based Packet Marking (CLI)

This procedure explains how to configure the following class-based packet marking features on your switch:

- CoS value
- DSCP value
- IP value
- Precedence value
- QoS group value
- WLAN value

Before you begin

You should have created a class map and a policy map before beginning this procedure.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

Step 2	**policy-map** *policy name*
	Example:
	`Switch(config)# policy-map policy1`
	`Switch(config-pmap)#`
		Enters policy map configuration mode.
		Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

Step 3	**class** *class name*
	Example:
	`Switch(config-pmap)# class class1`
	`Switch(config-pmap-c)#`
		Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change.
		Command options for policy class map configuration mode include the following:
		• **admit**—Admits the request for Call Admission Control (CAC).
		• **bandwidth**—Bandwidth configuration options.
		• **exit**—Exits from the QoS class action configuration mode.
		• **no**—Negates or sets default values for the command.
		• **police**—Policer configuration options.

	Command or Action	Purpose

		• **priority**—Strict scheduling priority configuration options for this class.
		• **queue-buffers**—Queue buffer configuration options.
		• **queue-limit**—Queue maximum threshold for Weighted Tail Drop (WTD) configuration options.
		• **service-policy**—Configures the QoS service policy.
		• **set**—Sets QoS values using the following options:
		  • CoS values
		  • DSCP values
		  • Precedence values
		  • QoS group values
		  • WLAN values
		• **shape**—Traffic-shaping configuration options.
		Note This procedure describes the available configurations using **set** command options. The other command options (**admit**, **bandwidth**, etc.) are described in other sections of this guide. Although this task lists all of the possible **set** commands, only one **set** command is supported per class.

Step 4	**set cos** {*cos value* | **cos table** *table-map name* | **dscp table** *table-map name* | **precedence table** *table-map name* | **qos-group table** *table-map name* | **wlan user-priority table** *table-map name*}
	Example:
	`Switch(config-pmap)# set cos 5`
	`Switch(config-pmap)#`
		(Optional) Sets the specific IEEE 802.1Q Layer 2 CoS value of an outgoing packet. Values are from 0 to7.
		You can also set the following values using the **set cos** command:
		• **cos table**—Sets the CoS value based on a table map.
		• **dscp table**—Sets the code point value based on a table map.
		• **precedence table**—Sets the code point value based on a table map.

	Command or Action	Purpose
		• **qos-group table**—Sets the CoS value from QoS group based on a table map. • **wlan user-priority table**—Sets the CoS value from the WLAN user priority based on a table map.

Step 5	**set dscp** {*dscp value* | **default** | **dscp table** *table-map name* | **ef** | **precedence table** *table-map name* | **qos-group table** *table-map name* | **wlan user-priority table** *table-map name*}
	Example:
	`Switch(config-pmap)# set dscp af11`
	`Switch(config-pmap)#`
		(Optional) Sets the DSCP value.
		In addition to setting specific DSCP values, you can also set the following using the **set dscp** command:
		• **default**—Matches packets with default DSCP value (000000).
		• **dscp table**—Sets the packet DSCP value from DSCP based on a table map.
		• **ef**—Matches packets with EF DSCP value (101110).
		• **precedence table**—Sets the packet DSCP value from precedence based on a table map.
		• **qos-group table**—Sets the packet DSCP value from a QoS group based upon a table map.
		• **wlan user-priority table**—Sets the packet DSCP value based upon a WLAN user-priority based upon a table map.

Step 6	**set ip** {**dscp** | **precedence**}
	Example:
	`Switch(config-pmap)# set ip dscp c3`
	`Switch(config-pmap)#`
		(Optional) Sets IP specific values. These values are either IP DSCP or IP precedence values.
		You can set the following values using the **set ip dscp** command:
		• *dscp value*—Sets a specific DSCP value.
		• **default**—Matches packets with default DSCP value (000000).
		• **dscp table**—Sets the packet DSCP value from DSCP based on a table map.
		• **ef**—Matches packets with EF DSCP value (101110).
		• **precedence table**—Sets the packet DSCP value from precedence based on a table map.

	Command or Action	Purpose
		• **qos-group table**—Sets the packet DSCP value from a QoS group based upon a table map. • **wlan user-priority table**—Sets the packet DSCP value based upon a WLAN user-priority based upon a table map. You can set the following values using the **set ip precedence** command: • *precedence value*—Sets the precedence value (from 0 to 7) . • **cos table**—Sets the packet precedence value from Layer 2 CoS based on a table map. • **dscp table**—Sets the packet precedence from DSCP value based on a table map. • **precedence table**—Sets the precedence value from precedence based on a table map • **qos-group table**—Sets the precedence value from a QoS group based upon a table map.

Step 7	**set precedence** {*precedence value* | **cos table** *table-map name* | **dscp table** *table-map name* | **precedence table** *table-map name* | **qos-group table** *table-map name*}
	Example:
	`Switch(config-pmap)# set precedence 5`
	`Switch(config-pmap)#`
		(Optional) Sets precedence values in IPv4 and IPv6 packets.
		You can set the following values using the **set precedence** command:
		• *precedence value*—Sets the precedence value (from 0 to 7) .
		• **cos table**—Sets the packet precedence value from Layer 2 CoS on a table map.
		• **dscp table**—Sets the packet precedence from DSCP value on a table map.
		• **precedence table**—Sets the precedence value from precedence based on a table map.
		• **qos-group table**—Sets the precedence value from a QoS group based upon a table map.

	Command or Action	Purpose

Step 8	**set qos-group** {*qos-group value* | **dscp table** *table-map name* | **precedence table** *table-map name*}
	Example:
	`Switch(config-pmap)# set qos-group 10`
	`Switch(config-pmap)#`
		(Optional) Sets QoS group values. You can set the following values using this command:
		• *qos-group value*—A number from 1 to 31.
		• **dscp table**—Sets the code point value from DSCP based on a table map.
		• **precedence table**—Sets the code point value from precedence based on a table map.

Step 9	**set wlan user-priority** {*wlan user-priority value* | **cos table** *table-map name* | **dscp table** *table-map name* | **qos-group table** *table-map name* | **wlan table** *table-map name*}
	Example:
	`Switch(config-pmap)# set wlan user-priority 1`
	`Switch(config-pmap)#`
		(Optional) Sets the WLAN user priority value. You can set the following values using this command:
		• *wlan user-priority value*—A value between 0 to 7.
		• **cos table**—Sets the WLAN user priority value from CoS based on a table map.
		• **dscp table**—Sets the WLAN user priority value from DSCP based on a table map.
		• **qos-group table**—Sets the WLAN user priority value from QoS group based on a table map.
		• **wlan table**—Sets the WLAN user priority value from the WLAN user priority based on a table map.

Step 10	**end**
	Example:
	`Switch(config-pmap)# end`
	`Switch#`
		Saves configuration changes.

Step 11	**show policy-map** **Example:** `Switch# show policy-map`	(Optional) Displays policy configuration information for all classes configured for all service policies.

What to do next

Attach the traffic policy to an interface using the **service-policy** command.

Configuring Class Maps for Voice and Video (CLI)

To configure class maps for voice and video traffic, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**class-map** *class-map-name* **Example:** `Switch(config)# class-map voice`	Creates a class map.
Step 2	**match dscp** *dscp-value-for-voice* **Example:** `Switch(config-cmap)# match dscp 46`	Matches the DSCP value in the IPv4 and IPv6 packets. Set this value to 46.
Step 3	**class-map** *class-map-name* **Example:** `Switch(config)# class-map video`	Configures a class map.
Step 4	**match dscp** *dscp-value-for-video* **Example:** `Switch(config-cmap)# match dscp 34`	Matches the DSCP value in the IPv4 and IPv6 packets. Set this value to 34.

Attaching a Traffic Policy to an Interface (CLI)

After the traffic class and traffic policy are created, you must use the **service-policy** interface configuration command to attach a traffic policy to an interface, and to specify the direction in which the policy should be applied (either on packets coming into the interface or packets leaving the interface).

Before you begin

A traffic class and traffic policy must be created before attaching a traffic policy to an interface.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *type* **Example:** `Switch(config)# interface GigabitEthernet1/0/1`	Enters interface configuration mode and configures an interface. Command parameters for the interface configuration include: • **Auto Template**— Auto-template interface

	Command or Action	Purpose
	`Switch(config-if)#`	• **Capwap**—CAPWAP tunnel interface • **GigabitEthernet**—Gigabit Ethernet IEEE 802 • **GroupVI**—Group virtual interface • **Internal Interface**— Internal interface • **Loopback**—Loopback interface • **Null**—Null interface • **Port-channel**—Ethernet Channel of interface • **TenGigabitEthernet**—10-Gigabit Ethernet • **Tunnel**—Tunnel interface • **Vlan**—Catalyst VLANs • **Range**—Interface range

Step 3	**service-policy** {**input** *policy-map* | **output** *policy-map* }
	Example:
	`Switch(config-if)# service-policy output policy_map_01`
	`Switch(config-if)#`
		Attaches a policy map to an input or output interface. This policy map is then used as the service policy for that interface.
		In this example, the traffic policy evaluates all traffic leaving that interface.

Step 4	**end**
	Example:
	`Switch(config-if)# end`
	`Switch#`
		Saves configuration changes.

Step 5	**show policy map** **Example:** `Switch# show policy map`	(Optional) Displays statistics for the policy on the specified interface.

What to do next

Proceed to attach any other traffic policy to an interface, and to specify the direction in which the policy should be applied.

Related Topics

Policy Map on Physical Port, on page 609

Configuring SSID Policies (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless**.

Step 2 Expand the **QoS** node by clicking on the left pane and choose **QOS-Policy**.

The **Create QoS Policy** page is displayed.

Step 3 Click **Add New** to create a new QoS Policy.

The **QoS Policy** page is displayed.

Step 4 Select **SSID** from the **Policy Type** drop-down menu.

Step 5 Select the direction into which the policy needs to be applied from the **Policy Direction** drop-down list.

The available options are:

- **Ingress**
- **Egress**

Note Voice and video configurations are available only in the egress direction.

Note When creating an egress SSID policy for voice and video classes, if the **port_child_policy** is already configured with voice and video classes having priority level, the existing **port_child_policy** is used. If a **port_child_policy** does not exist with voice and video classes, the switch will create voice and video classes with priority levels 1 and 2 under **port_child_policy** for voice and video traffic.

Step 6 Specify a policy name in the **Policy Name** text box.

Step 7 Provide a description to the policy in the **Description** text box.

Step 8 Select the trust parameter from the **Trust** drop-down list.

The following options are available:

- **DSCP**— Assigns a label to indicate the given quality of service as DSCP.
- **COS**—Matches IEEE 802.1Q class of service. This option is not available when the **Policy Direction** is ingress.
- **User Priority**—Enter the 802.11e user priority. This option is not available when the **Policy Direction** is egress.
- **None**—This option is available when the **Policy Direction** is egress. This option is available only for egress policies.

Step 9 If you chose **Egress** policy above, the following options are available:

- **Bandwidth**—Specifies the bandwidth rate. The following options are available:
  - **Rate**—Specifies the bandwidth in kbps. Enter a value in kbps in the **Value** field.
  - **Remaining Ratio**—Specifies the bandwidth in BRR (bandwidth remaining ratio). Enter the percentage in the **Percent** field.

Note If you choose the **Rate** option for the **Bandwidth** parameter, this value must be greater than the sum of the policing values for voice and video traffic.

.

- **Enable Voice**—Check the **Enable Voice** check box to enable voice traffic on this policy. Specify the following properties:
  - **Priority**—Sets the priority for this policy for strict scheduling. The priority level is set to 1.
  - **Police (kbps)**—Specifies the police rate in Kilobits per second.
  - **CAC**—Enables or disables CAC. If CAC is enabled, you must specify the following options:
    - **User priority**This option is available when the **Policy Direction** is ingress. Enter the 802.11e user priority. The range is from 0 to 7. By default, a value of 6 is assigned.
    - **Rate(kbps)**

      Note The CAC rate must be less than the police rate.

- **Enable Video**—Check the **Enable Video** check box to enable video traffic on this policy. Specify the following properties:
- **Priority**—Sets the priority for this policy for strict scheduling.
- **Police (kbps)—**Specifies the police rate in kilobits per second.

Step 10 Click **Apply**.

Related Topics

SSID Policies, on page 598
Supported QoS Features on Wireless Targets, on page 594
Examples: SSID Policy
Examples: Configuring Downstream SSID Policy, on page 697

Applying an SSID or Client Policy on a WLAN (CLI)

Before you begin

You must have a service-policy map configured before applying it on an SSID.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.

	Command or Action	Purpose
Step 3	**service-policy** [**input** | **output**] *policy-name* **Example:** `Switch(config-wlan)# service-policy input policy-map-ssid`	Applies the policy. The following options are available: • **input**— Assigns the policy map to WLAN ingress traffic. • **output**— Assigns the policy map to WLAN egress traffic.
Step 4	**service-policy client** [**input** | **output**] *policy-name* **Example:** `Switch(config-wlan)# service-policy client input policy-map-client`	Applies the policy. The following options are available: • **input**— Assigns the client policy for ingress direction on the WLAN. • **output**— Assigns the client policy for egress direction on the WLAN.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

SSID Policies, on page 598
Supported QoS Features on Wireless Targets, on page 594
Examples: SSID Policy
Examples: Configuring Downstream SSID Policy, on page 697

Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps (CLI)

You can configure a nonhierarchical policy map on a physical port that specifies which traffic class to act on. Actions supported are remarking and policing.

Before you begin

You should have already decided upon the classification, policing, and marking of your network traffic by policy maps prior to beginning this procedure.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**class-map** {*class-map name* | **match-any** }	Enters class map configuration mode.

	Command or Action	Purpose

	Example:
	`Switch(config)# class-map ipclass1`
	`Switch(config-cmap)# exit`
	`Switch(config)#`
		• Creates a class map to be used for matching packets to the class whose name you specify.
		• If you specify **match-any**, one of the match criteria must be met for traffic entering the traffic class to be classified as part of the traffic class. This is the default.

Step 3	**match access-group** { *access list index* | *access list name* }
	Example:
	`Switch(config-cmap)# match access-group 1000`
	`Switch(config-cmap)# exit`
	`Switch(config)#`
		Specifies the classification criteria to match to the class map. You can match on the following criteria:
		• **access-group**—Matches to access group.
		• **class-map**—Matches to another class map.
		• **cos**—Matches to a CoS value.
		• **dscp**—Matches to a DSCP value.
		• **ip**—Matches to a specific IP value.
		• **non-client-nrt**—Matches non-client NRT.
		• **precedence**—Matches precedence in IPv4 and IPv6 packets.
		• **qos-group**—Matches to a QoS group.
		• **vlan**—Matches to a VLAN.

Step 4	**policy-map** *policy-map-name*
	Example:
	`Switch(config)# policy-map flowit`
	`Switch(config-pmap)#`
		Creates a policy map by entering the policy map name, and enters policy-map configuration mode.
		By default, no policy maps are defined.

Step 5	**class** {*class-map-name* | **class-default**}
	Example:
	`Switch(config-pmap)# class ipclass1`
	`Switch(config-pmap-c)#`
		Defines a traffic classification, and enter policy-map class configuration mode.
		By default, no policy map class-maps are defined.
		If a traffic class has already been defined by using the **class-map** global configuration command, specify its name for *class-map-name* in this command.
		A **class-default** traffic class is predefined and can be added to any policy. It is always placed

	Command or Action	Purpose
		at the end of a policy map. With an implied **match any** included in the **class-default** class, all packets that have not already matched the other traffic classes will match **class-default**.

Step 6	**set** {**cos** | **dscp** | **ip** | **precedence** | **qos-group** | **wlan user-priority**}
	Example:
	`Switch(config-pmap-c)# set dscp 45`
	`Switch(config-pmap-c)#`
		(Optional) Sets the QoS values. Possible QoS configuration values include:
		• **cos**—Sets the IEEE 802.1Q/ISL class of service/user priority.
		• **dscp**—Sets DSCP in IP(v4) and IPv6 packets.
		• **ip**—Sets IP specific values.
		• **precedence**—Sets precedence in IP(v4) and IPv6 packet.
		• **qos-group**—Sets QoS group.
		• **wlan user-priority**—Sets WLAN user priority.
		In this example, the **set dscp** command classifies the IP traffic by setting a new DSCP value in the packet.

Step 7	**police** {*target_bit_rate* | **cir** | **rate** }
	Example:
	`Switch(config-pmap-c)# police 100000 conform-action transmit exceed-action drop`
	`Switch(config-pmap-c)#`
		(Optional) Configures the policer:
		• *target_bit_rate*—Specifies the bit rate per second, enter a value between 8000 and 10000000000.
		• **cir**—Committed Information Rate.
		• **rate**—Specifies the police rate, PCR for hierarchical policies, or SCR for single-level ATM 4.0 policer policies.
		In this example, the **police** command adds a policer to the class where any traffic beyond the 100000 set target bit rate is dropped.

Step 8	**exit** **Example:** `Switch(config-pmap-c)# exit`	Returns to policy map configuration mode.
Step 9	**exit** **Example:**	Returns to global configuration mode.

	Command or Action	Purpose
	`Switch(config-pmap)# exit`	
Step 10	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 2/0/1`	Specifies the port to attach to the policy map, and enters interface configuration mode. Valid interfaces include physical ports.
Step 11	**service-policy input** *policy-map-name* **Example:** `Switch(config-if)# service-policy input flowit`	Specifies the policy-map name, and applies it to an ingress port. Only one policy map per ingress port is supported.
Step 12	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 13	**show policy-map** [*policy-map-name* [**class** *class-map-name*]] **Example:** `Switch# show policy-map`	(Optional) Verifies your entries.
Step 14	**copy running-config startup-config** **Example:** `Switch# copy-running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

If applicable to your QoS configuration, configure classification, policing, and marking of traffic on SVIs by using policy maps.

Classifying, Policing, and Marking Traffic on SVIs by Using Policy Maps (CLI)

Before you begin

You should have already decided upon the classification, policing, and marking of your network traffic by using policy maps prior to beginning this procedure.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**class-map** {*class-map name* | **match-any** } **Example:** `Switch(config)# class-map class_vlan100`	Enters class map configuration mode. • Creates a class map to be used for matching packets to the class whose name you specify. • If you specify **match-any**, one of the match criteria must be met for traffic entering the traffic class to be classified as part of the traffic class. This is the default.

Step 3	**match vlan** *vlan number*
	Example:
	`Switch(config-cmap)# match vlan 100`
	`Switch(config-cmap)# exit`
	`Switch(config)#`
		Specifies the VLAN to match to the class map.

Step 4	**policy-map** *policy-map-name*
	Example:
	`Switch(config)# policy-map policy_vlan100`
	`Switch(config-pmap)#`
		Creates a policy map by entering the policy map name, and enters policy-map configuration mode.
		By default, no policy maps are defined.

Step 5	**description** *description* **Example:** `Switch(config-pmap)# description vlan 100`	(Optional) Enters a description of the policy map.

Step 6	**class** {*class-map-name* | **class-default**}
	Example:
	`Switch(config-pmap)# class class_vlan100`
	`Switch(config-pmap-c)#`
		Defines a traffic classification, and enters the policy-map class configuration mode.
		By default, no policy map class-maps are defined.
		If a traffic class has already been defined by using the **class-map** global configuration

	Command or Action	Purpose
		command, specify its name for *class-map-name* in this command. A **class-default** traffic class is predefined and can be added to any policy. It is always placed at the end of a policy map. With an implied **match any** included in the **class-default** class, all packets that have not already matched the other traffic classes will match **class-default**.

Step 7	**set** {**cos** | **dscp** | **ip** | **precedence** | **qos-group** | **wlan user-priority**}
	Example:
	`Switch(config-pmap-c)# set dscp af23`
	`Switch(config-pmap-c)#`
		(Optional) Sets the QoS values. Possible QoS configuration values include:
		• **cos**—Sets the IEEE 802.1Q/ISL class of service/user priority.
		• **dscp**—Sets DSCP in IP(v4) and IPv6 packets.
		• **ip**—Sets IP specific values.
		• **precedence**—Sets precedence in IP(v4) and IPv6 packet.
		• **qos-group**—Sets QoS group.
		• **wlan user-priority**—Sets WLAN user-priority.
		In this example, the **set dscp** command classifies the IP traffic by matching the packets with a DSCP value of AF23 (010010).

Step 8	**police** {*target_bit_rate* | **cir** | **rate**}
	Example:
	`Switch(config-pmap-c)# police 200000 conform-action transmit exceed-action drop`
	`Switch(config-pmap-c)#`
		(Optional) Configures the policer:
		• *target_bit_rate*—Specifies the bit rate per second. Enter a value between 8000 and 10000000000.
		• **cir**—Committed Information Rate.
		• **rate**—Specifies the police rate, PCR for hierarchical policies, or SCR for single-level ATM 4.0 policer policies.
		In this example, the **police** command adds a policer to the class where any traffic beyond the 200000 set target bit rate is dropped.

Step 9	**exit** **Example:** `Switch(config-pmap-c)# exit`	Returns to policy map configuration mode.

	Command or Action	Purpose
Step 10	**exit** **Example:** `Switch(config-pmap)# exit`	Returns to global configuration mode.
Step 11	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/3`	Specifies the port to attach to the policy map, and enters interface configuration mode. Valid interfaces include physical ports.
Step 12	**service-policy input** *policy-map-name* **Example:** `Switch(config-if)# service-policy input policy_vlan100`	Specifies the policy-map name, and applies it to an ingress port. Only one policy map per ingress port is supported.
Step 13	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 14	**show policy-map** [*policy-map-name* [**class** *class-map-name*]] **Example:** `Switch# show policy-map`	(Optional) Verifies your entries.
Step 15	**copy running-config startup-config** **Example:** `Switch# copy-running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Policy Map on VLANs, on page 609
Examples: Policer VLAN Configuration, on page 704

Configuring Table Maps (CLI)

Table maps are a form of marking, and also enable the mapping and conversion of one field to another using a table. For example, a table map can be used to map and convert a Layer 2 CoS setting to a precedence value in Layer 3.

Note A table map can be referenced in multiple policies or multiple times in the same policy.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

Step 2	**table-map** *name* {**default** {*default value* | **copy** | **ignore**} | **exit** | **map** {**from** *from value* **to** *to value* } | **no**}
	Example:
	`Switch(config)# table-map table01`
	`Switch(config-tablemap)#`
		Creates a table map and enters the table map configuration mode. In table map configuration mode, you can perform the following tasks:
		• **default**—Configures the table map default value, or sets the default behavior for a value not found in the table map to copy or ignore.
		• **exit**—Exits from the table map configuration mode.
		• **map**—Maps a *from* to a *to* value in the table map.
		• **no**—Negates or sets the default values of the command.

Step 3	**map from** *value* **to** *value*
	Example:
	`Switch(config-tablemap)# map from 0 to 2`
	`Switch(config-tablemap)# map from 1 to 4`
	`Switch(config-tablemap)# map from 24 to 3`
	`Switch(config-tablemap)# map from 40 to 6`
	`Switch(config-tablemap)# default 0`
	`Switch(config-tablemap)#`
		In this step, packets with DSCP values 0 are marked to the CoS value 2, DSCP value 1 to the CoS value 4, DSCP value 24 to the CoS value 3, DSCP value 40 to the CoS value 6 and all others to the CoS value 0.
		Note The mapping from CoS values to DSCP values in this example is configured by using the **set** policy map class configuration command as described in a later step in this procedure.

Step 4	**exit**
	Example:
	`Switch(config-tablemap)# exit`
	`Switch(config)#`
		Returns to global configuration mode.

	Command or Action	Purpose

Step 5	**exit**
	Example:
	`Switch(config) exit`
	`Switch#`
		Returns to privileged EXEC mode.

Step 6	**show table-map**
	Example:
	`Switch# show table-map`
	`Table Map table01`
	`from 0 to 2`
	`from 1 to 4`
	`from 24 to 3`
	`from 40 to 6`
	`default 0`
		Displays the table map configuration.

Step 7	**configure terminal**
	Example:
	`Switch# configure terminal`
	`Switch(config)#`
		Enters global configuration mode.

Step 8	**policy-map**
	Example:
	`Switch(config)# policy-map table-policy`
	`Switch(config-pmap)#`
		Configures the policy map for the table map.

Step 9	**class class-default**
	Example:
	`Switch(config-pmap)# class class-default`
	`Switch(config-pmap-c)#`
		Matches the class to the system default.

Step 10	**set cos dscp table** *table map name*
	Example:
	`Switch(config-pmap-c)# set cos dscp table table01`
	`Switch(config-pmap-c)#`
		If this policy is applied on input port, that port will have trust DSCP enabled on that port and marking will take place depending upon the specified table map.

Step 11	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Switch(config-pmap-c)# end` `Switch#`	

What to do next

Configure any additional policy maps for QoS for your network. After creating your policy maps, attach the traffic policy or polices to an interface using the **service-policy** command.

Related Topics

Table Map Marking, on page 612
Examples: Table Map Marking Configuration, on page 706

Configuring Trust

Configuring Trust Behavior for Wireless Traffic (CLI)

The Cisco IOS XE 3.2 Release supported different trust defaults for wired and wireless ports. The trust default for wired ports was the same as for this software release. For wireless ports, the default system behavior was non-trust, which meant that when the switch came up, all markings for the wireless ports were defaulted to zero and no traffic received priority treatment. For compatibility with an existing wired switch, all traffic went to the best-effort queue by default. The access point performed priority queuing by default. In the downstream direction, the access point maintained voice, video, best-effort, and background queues for queuing. The access selected the queuing strategy based on the 11e tag information. By default, the access point treated all wireless packets as best effort.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**qos wireless-default-untrust** **Example:** `Switch (config)# qos wireless-default-untrust`	Configures the behavior of the switch to untrust wireless traffic. To configure the switch to trust wireless traffic by default, use the **no** form of the command.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Trust Behavior for Wired and Wireless Ports, on page 621

Configuring QoS Features and Functionality

Configuring Call Admission Control (CLI)

This task explains how to configure class-based, unconditional packet marking features on your switch for Call Admission Control (CAC).

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

Step 2	**class-map** *class name*
	Example:
	`Switch(config)# class-map voice`
	`Switch(config-cmap)#`
		Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:
		• *word*—Class map name.
		• **class-default**—System default class matching any otherwise unclassified packets.

Step 3	**match dscp** *dscp value* **Example:** `Switch(config-cmap)#  match dscp 46`	(Optional) Matches the DSCP values in IPv4 and IPv6 packets.

Step 4	**exit**
	Example:
	`Switch(config-cmap)# exit`
	`Switch(config)#`
		Returns to global configuration mode.

Step 5	**class-map** *class name*
	Example:
	`Switch(config)# class-map video`
	`Switch(config-cmap)#`
		Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:
		• *word*—Class map name.
		• **class-default**—System default class matching any otherwise unclassified packets.

	Command or Action	Purpose
Step 6	**match dscp** *dscp value* **Example:** `Switch(config-cmap)# match dscp 34`	(Optional) Matches the DSCP values in IPv4 and IPv6 packets.

Step 7	**exit**
	Example:
	`Switch(config-cmap)# exit`
	`Switch(config)#`
		Returns to global configuration mode.

Step 8	**table-map** *name*
	Example:
	`Switch(config)# table-map dscp2dscp`
	`Switch(config-tablemap)#`
		Creates a table map and enters the table map configuration mode.

Step 9	**default copy** **Example:** `Switch(config-tablemap)# default copy`	Sets the default behavior for value not found in the table map to copy. **Note** This is the default option. You can also do a mapping of values for DSCP to DSCP.

Step 10	**exit**
	Example:
	`Switch(config-tablemap)# exit`
	`Switch(config)#`
		Returns to global configuration mode.

Step 11	**table-map** *name*
	Example:
	`Switch(config)# table-map dscp2up`
	`Switch(config-tablemap)#`
		Creates a new table map and enters the table map configuration mode.

Step 12	**default copy** **Example:** `Switch(config-tablemap)# default copy`	Sets the default behavior for value not found in the table map to copy. **Note** This is the default option. You can also do a mapping of values for DSCP to UP.
Step 13	**exit** **Example:**	Returns to global configuration mode.

	Command or Action	Purpose
	`Switch(config-tablemap)# exit` `Switch(config)#`	

Step 14	**policy-map** *policy name*
	Example:
	`Switch(config)# policy-map ssid_child_cac`
	`Switch(config-pmap)#`
		Enters policy map configuration mode.
		Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

Step 15	**class** *class-map-name* **Example:** `Switch(config-pmap)# class voice`	Defines an interface-level traffic classification, and enters policy-map configuration mode.
Step 16	**priority level** *level_value* **Example:** `Switch(config-pmap-c)# priority level 1`	The **priority** command assigns a strict scheduling priority for the class. **Note** Priority level 1 is more important than priority level 2. Priority level 1 reserves bandwidth that is processed first for QoS, so its latency is very low. Both priority level 1 and 2 reserve bandwidth.
Step 17	**police** [*target_bit_rate* | **cir** | **rate**] **Example:** `Switch(config-pmap-c)# police cir 10m`	(Optional) Configures the policer: • *target_bit_rate*—Specifies the bit rate per second. Enter a value between 8000 and 10000000000. • **cir**—Committed Information Rate. • **rate**—Specifies the police rate, PCR for hierarchical policies, or SCR for single-level ATM 4.0 policer policies.

Step 18	**admit cac wmm-tspec**
	Example:
	`Switch(config-pmap-c)# admit cac wmm-tspec`
	`Switch(config-pmap-cac-wmm)#`
		Configures call admission control for the policy map.
		Note This command only configures CAC for wireless QoS.

Step 19	**rate** *value* **Example:**	Configures the target bit rate (Kilo Bits per second). Enter a value from 8 to 10000000.

	Command or Action	Purpose
	`Switch(config-pmap-admit-cac-wmm)# rate 5000`	
Step 20	**wlan-up** *value* **Example:** `Switch(config-pmap-admit-cac-wmm)# wlan-up 6 7`	Configures the WLAN UP value. Enter a value from 0 to 7.

Step 21	**exit**
	Example:
	`Switch(config-pmap-admit-cac-wmm)# exit`
	`Switch(config-pmap-c)#`
		Returns to policy map class configuration mode.

Step 22	**exit**
	Example:
	`Switch(config-pmap-c)# exit`
	`Switch(config-pmap)#`
		Returns to policy map configuration mode.

Step 23	**class** *class name*
	Example:
	`Switch(config-pmap)# class video`
	`Switch(config-pmap-c)#`
		Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:
		• *word*—Class map name.
		• **class-default**—System default class matching any otherwise unclassified packets.

Step 24	**priority level** *level_value* **Example:** `Switch(config-pmap-c)# priority level 2`	The **priority** command assigns a strict scheduling priority for the class. **Note** Priority level 1 is more important than priority level 2. Priority level 1 reserves bandwidth that is processed first for QoS, so its latency is very low. Both priority level 1 and 2 reserve bandwidth.
Step 25	**police** [*target_bit_rate* | **cir** | **rate**] **Example:** `Switch(config-pmap-c)# police cir 20m`	(Optional) Configures the policer: • *target_bit_rate*—Specifies the bit rate per second. Enter a value between 8000 and 10000000000.

	Command or Action	Purpose
		• **cir**—Committed Information Rate. • **rate**—Specifies the police rate, PCR for hierarchical policies, or SCR for single-level ATM 4.0 policer policies.

Step 26	**admit cac wmm-tspec**
	Example:
	`Switch(config-pmap-c)# admit cac wmm-tspec`
	`Switch(config-pmap-admit-cac-wmm)#`
		Configures call admission control for the policy map.
		Note This command only configures CAC for wireless QoS.

Step 27	**rate** *value* **Example:** `Switch(config-pmap-admit-cac-wmm)# rate 5000`	Configures the target bit rate (Kilo Bits per second). Enter a value from 8 to 10000000.
Step 28	**wlan-up** *value* **Example:** `Switch(config-pmap-admit-cac-wmm)# wlan-up 4 5`	Configures the WLAN UP value. Enter a value from 0 to 7.

Step 29	**exit**
	Example:
	`Switch(config-pmap-cac-wmm)# exit`
	`Switch(config-pmap)#`
		Returns to policy map configuration mode.

Step 30	**exit**
	Example:
	`Switch(config-pmap)# exit`
	`Switch(config)#`
		Returns to global configuration mode.

Step 31	**policy-map** *policy name*
	Example:
	`Switch(config)# policy-map ssid_cac`
	`Switch(config-pmap)#`
		Enters policy map configuration mode.
		Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

	Command or Action	Purpose
Step 32	**class** *class-map-name* **Example:** `Switch(config-pmap)# class default`	Defines an interface-level traffic classification, and enters policy-map configuration mode. In this example, the class map is set to default.
Step 33	**set dscp dscp table** *table_map_name* **Example:** `Switch(config-pmap-c)# set dscp dscp table dscp2dscp`	(Optional) Sets the QoS values. In this example, the **set dscp dscp table** command creates a table map and sets its values.
Step 34	**set wlan user-priority dscp table** *table_map_name* **Example:** `Switch(config-pmap-c)# set wlan user-priority dscp table dscp2up`	(Optional) Sets the QoS values. In this example, the **set wlan user-priority dscp table** command sets the WLAN user priority.
Step 35	**shape average** {*target bit rate* | **percent** *percentage*} **Example:** `Switch(config-pmap-c)# shape average 100000000`	Configures the average shape rate. You can configure the average shape rate by target bit rates (bits per second) or by percentage of interface bandwidth for the Committed Information Rate (CIR).
Step 36	**queue-buffers** {**ratio** *ratio value*} **Example:** `Switch(config-pmap-c)# queue-buffers ratio 0`	Configures the relative buffer size for the queue. **Note** The sum of all configured buffers in a policy must be less than or equal to 100 percent. Unallocated buffers are evenly distributed to all the remaining queues. Ensure sufficient buffers are allocated to all queues including the priority queues. **Note** Protocol Data Units (PDUs) for network control protocols such as spanning-tree and LACP utilize the priority queue or queue 0 (when a priority queue is not configured). Ensure sufficient buffers are allocated to these queues for the protocols to function.

	Command or Action	Purpose
Step 37	**service-policy** *policy_map_name* **Example:** `Switch(config-pmap-c)# service-policy ssid_child_cac`	Specifies the policy map for the service policy.

Step 38	**end**
	Example:
	`Switch(config-pmap)# end`
	`Switch#`
		Saves configuration changes.

Step 39	**show policy-map** **Example:** `Switch# show policy-map`	(Optional) Displays policy configuration information for all classes configured for all service policies.

What to do next

Configure any additional policy maps for QoS for your network. After creating your policy maps, attach the traffic policy or polices to an interface using the **service-policy** command.

For additional information about CAC, refer to the *System Management Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*.

For additional information about CAC, refer to the *System Management Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)* .

Configuring Bandwidth (CLI)

This procedure explains how to configure bandwidth on your switch.

Before you begin

You should have created a class map for bandwidth before beginning this procedure.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**policy-map** *policy name*	Enters policy map configuration mode.

	Command or Action	Purpose

	Example:
	
	`Switch(config)# policy-map policy_bandwidth01`
	`Switch(config-pmap)#`
		Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

Step 3	**class** *class name*
	Example:
	
	`Switch(config-pmap)# class class_bandwidth01`
	`Switch(config-pmap-c)#`
		Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:
		• *word*—Class map name.
		• **class-default**—System default class matching any otherwise unclassified packets.

Step 4	**bandwidth** {*Kb/s* | **percent** *percentage* | **remaining** { **ratio** *ratio* }}
	Example:
	
	`Switch(config-pmap-c)# bandwidth 200000`
	`Switch(config-pmap-c)#`
		Configures the bandwidth for the policy map. The parameters include:
		• *Kb/s*—Configures a specific value in kilobits per second (from 20000 to 10000000).
		• **percent-**—Allocates minimum bandwidth to a particular class based on a percentage. The queue can oversubscribe bandwidth in case other queues do not utilize the entire port bandwidth. The total sum cannot exceed 100 percent, and in case it is less than 100 percent, the rest of the bandwidth is equally divided along all bandwidth queues.
		• **remaining**— Allocates minimum bandwidth to a particular class. The queue can oversubscribe bandwidth in case other queues do not utilize entire port bandwidth. The total sum cannot exceed 100 percent. It is preferred to use this command when the **priority** command is used for certain queues in the policy. You can also assign ratios rather than percentages to each queue; the queues will be assigned certain weights which are inline with these ratios. Ratios can range from 0 to 100. Total bandwidth ratio allocation for the policy in this case can exceed 100.

	Command or Action	Purpose
		Note You cannot mix bandwidth types on a policy map. For example, you cannot configure bandwidth in a single policy map using both a bandwidth percent and in kilobits per second.

Step 5	**end**
	Example:
	`Switch(config-pmap-c)# end`
	`Switch#`
		Saves configuration changes.

Step 6	**show policy-map** **Example:** `Switch# show policy-map`	(Optional) Displays policy configuration information for all classes configured for all service policies.

What to do next

Configure any additional policy maps for QoS for your network. After creating the policy maps, attach the traffic policy or polices to an interface using the **service-policy** command.

Related Topics

Bandwidth, on page 617

Configuring Police (CLI)

This procedure explains how to configure policing on your switch.

Before you begin

You should have created a class map for policing before beginning this procedure.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**policy-map** *policy name* **Example:** `Switch(config)# policy-map`	Enters policy map configuration mode. Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

	Command or Action	Purpose
	policy_police01 Switch(config-pmap)#	
Step 3	**class** *class name* **Example:** Switch(config-pmap)# **class class_police01** Switch(config-pmap-c)#	Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following: • *word*—Class map name. • **class-default**—System default class matching any otherwise unclassified packets.
Step 4	**police** {*target_bit_rate* [*burst bytes* | **bc** | **conform-action** | **pir**] | **cir** {*target_bit_rate* | **percent** *percentage*} | **rate** {*target_bit_rate* | **percent** *percentage*} **conform-action transmit exceed-action** {**drop** [**violate action**] | **set-cos-transmit** | **set-dscp-transmit** | **set-prec-transmit** | **transmit** [**violate action**] }} **Example:** Switch(config-pmap-c)# **police 8000 conform-action transmit exceed-action drop** Switch(config-pmap-c)#	The following **police** subcommand options are available: • *target_bit_rate*—Bits per second (from 8000 to 10000000000). • *burst bytes*—Enter a value from 1000 to 512000000. • **bc**—Conform burst. • **conform-action**—Action taken when rate is less than conform burst. • **pir**—Peak Information Rate. • **cir**—Committed Information Rate. • *target_bit_rate*—Target bit rate (8000 to10000000000). • **percent**—Percentage of interface bandwidth for CIR. • **rate**—Specifies the police rate, PCR for hierarchical policies, or SCR for single-level ATM 4.0 policer policies. • *target_bit_rate*—Target Bit Rate (8000 to 10000000000). • **percent**—Percentage of interface bandwidth for rate. The following **police conform-action transmit exceed-action** subcommand options are available: • **drop**—Drops the packet.

	Command or Action	Purpose
		• **set-cos-transmit**—Sets the CoS value and sends it. • **set-dscp-transmit**—Sets the DSCP value and sends it. • **set-prec-transmit**—Rewrites the packet precedence and sends it. • **transmit**—Transmits the packet. **Note** Policer-based markdown actions are only supported using table maps. Only one markdown table map is allowed for each marking field in the switch.

Step 5	**end**
	Example:
	`Switch(config-pmap-c)# end`
	`Switch#`
		Saves configuration changes.

Step 6	**show policy-map** **Example:** `Switch# show policy-map`	(Optional) Displays policy configuration information for all classes configured for all service policies.

What to do next

Configure any additional policy maps for QoS for your network. After creating your policy maps, attach the traffic policy or polices to an interface using the **service-policy** command.

Related Topics

Single-Rate Two-Color Policing, on page 614
Examples: Single-Rate Two-Color Policing Configuration, on page 705
Dual-Rate Three-Color Policing, on page 615
Examples: Dual-Rate Three-Color Policing Configuration, on page 705
Policing, on page 610
Token-Bucket Algorithm, on page 611
Examples: Policing Action Configuration, on page 703
Examples: Policing Units, on page 704

Configuring Priority (CLI)

This procedure explains how to configure priority on your switch.

The switch supports giving priority to specified queues. There are two priority levels available (1 and 2).

Note Queues supporting voice and video should be assigned a priority level of 1.

Before you begin

You should have created a class map for priority before beginning this procedure.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

Step 2	**policy-map** *policy name*
	Example:
	`Switch(config)# policy-map policy_priority01`
	`Switch(config-pmap)#`
		Enters policy map configuration mode.
		Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

Step 3	**class** *class name*
	Example:
	`Switch(config-pmap)# class class_priority01`
	`Switch(config-pmap-c)#`
		Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:
		• *word*—Class map name.
		• **class-default**—System default class matching any otherwise unclassified packets.

Step 4	**priority** [*Kb/s* [*burst_in_bytes*] | **level** *level_value* [*Kb/s* [*burst_in_bytes*] | **percent** *percentage* [*burst_in_bytes*]] | **percent** *percentage* [*burst_in_bytes*]]
	Example:
	`Switch(config-pmap-c)# priority level 1`
	`Switch(config-pmap-c)#`
		(Optional) The **priority** command assigns a strict scheduling priority for the class.
		The command options include:
		• *Kb/s*—Specifies the kilobits per second (from 1 to 2000000).
		• *burst_in_bytes*—Specifies the burst in bytes (from 32 to 2000000).
		• **level** *level_value*—Specifies the multilevel (1-2) priority queue.
		• *Kb/s*—Specifies the kilobits per second (from 1 to 2000000).

	Command or Action	Purpose
		• *burst_in_bytes*—Specifies the burst in bytes (from 32 to 2000000). • **percent**—Percentage of the total bandwidth. • *burst_in_bytes*—Specifies the burst in bytes (from 32 to 2000000). • **percent**—Percentage of the total bandwidth. • *burst_in_bytes*—Specifies the burst in bytes (32 to 2000000). **Note** Priority level 1 is more important than priority level 2. Priority level 1 reserves bandwidth that is processed first for QoS, so its latency is very low. Both priority level 1 and 2 reserve bandwidth.

Step 5	**end**
	Example:
	`Switch(config-pmap-c)# end`
	`Switch#`
		Saves configuration changes.

Step 6	**show policy-map** **Example:** `Switch# show policy-map`	(Optional) Displays policy configuration information for all classes configured for all service policies.

What to do next

Configure any additional policy maps for QoS for your network. After creating your policy maps, attach the traffic policy or polices to an interface using the **service-policy** command.

Related Topics

Priority Queues, on page 619

Configuring Queues and Shaping

Configuring Egress Queue Characteristics

Depending on the complexity of your network and your QoS solution, you may need to perform all of the procedures in this section. You need to make decisions about these characteristics:

- Which packets are mapped by DSCP, CoS, or QoS group value to each queue and threshold ID?
- What drop percentage thresholds apply to the queues, and how much reserved and maximum memory is needed for the traffic type?
- How much of the fixed buffer space is allocated to the queues?
- Does the bandwidth of the port need to be rate limited?
- How often should the egress queues be serviced and which technique (shaped, shared, or both) should be used?

Note You can only configure the egress queues on the switch.

Configuring Queue Buffers (CLI)

The switch allows you to allocate buffers to queues. If there is no allocation made to buffers, then they are divided equally for all queues. You can use the queue-buffer ratio to divide it in a particular ratio. Since by default DTS (Dynamic Threshold and Scaling) is active on all queues, these are soft buffers.

Note The queue-buffer ratio is supported on both wired and wireless ports, but the queue-buffer ratio cannot be configured with a queue-limit.

Before you begin

The following are prerequisites for this procedure:

- You should have created a class map for the queue buffer before beginning this procedure.
- You must have configured either bandwidth, shape, or priority on the policy map prior to configuring the queue buffers.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose

Step 2	**policy-map** *policy name*
	Example:
	`Switch(config)# policy-map policy_queuebuffer01`
	`Switch(config-pmap)#`
		Enters policy map configuration mode.
		Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

Step 3	**class** *class name*
	Example:
	`Switch(config-pmap)# class class_queuebuffer01`
	`Switch(config-pmap-c)#`
		Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:
		• *word*—Class map name.
		• **class-default**—System default class matching any otherwise unclassified packets.

Step 4	**bandwidth** {*Kb/s* | **percent** *percentage* | **remaining** { **ratio** *ratio value* }}
	Example:
	`Switch(config-pmap-c)# bandwidth percent 80`
	`Switch(config-pmap-c)#`
		Configures the bandwidth for the policy map. The command parameters include:
		• *Kb/s*—Use this command to configure a specific value. The range is 20000 to 10000000.
		• **percent**—Allocates a minimum bandwidth to a particular class using a percentage. The queue can oversubscribe bandwidth in case other queues do not utilize the entire port bandwidth. The total sum cannot exceed 100 percent, and in case it is less than 100 percent, the rest of the bandwidth is equally divided along all bandwidth queues.
		• **remaining**—Allocates a minimum bandwidth to a particular class. The queue can oversubscribe bandwidth in case other queues do not utilize entire port bandwidth. The total sum cannot exceed 100 percent. It is preferred to use this command when the **priority** command is used for certain queues in the policy. You can also assign ratios rather than a percentage to each queue; the queues will be assigned certain weights that are inline with these ratios. Ratios can range from 0 to 100. Total bandwidth ratio allocation for the policy in this case can exceed 100.

	Command or Action	Purpose
		Note You cannot mix bandwidth types on a policy map.

Step 5	**queue-buffers** {**ratio** *ratio value*}
	Example:
	`Switch(config-pmap-c)# queue-buffers ratio 10`
	`Switch(config-pmap-c)#`
		Configures the relative buffer size for the queue.
		Note The sum of all configured buffers in a policy must be less than or equal to 100 percent. Unallocated buffers are are evenly distributed to all the remaining queues. Ensure sufficient buffers are allocated to all queues including the priority queues.
		Note Protocol Data Units(PDUs) for network control protocols such as spanning-tree and LACP utilize the priority queue or queue 0 (when a priority queue is not configured). Ensure sufficient buffers are allocated to these queues for the protocols to function.

Step 6	**end**
	Example:
	`Switch(config-pmap-c)# end`
	`Switch#`
		Saves configuration changes.

Step 7	**show policy-map** **Example:** `Switch# show policy-map`	(Optional) Displays policy configuration information for all classes configured for all service policies.

What to do next

Configure any additional policy maps for QoS for your network. After creating your policy maps, attach the traffic policy or polices to an interface using the **service-policy** command.

Related Topics

Queue Buffer Allocation, on page 620
Examples: Queue Buffers Configuration, on page 703

Configuring Queue Limits (CLI)

You use queue limits to configure Weighted Tail Drop (WTD). WTD ensures the configuration of more than one threshold per queue. Each class of service is dropped at a different threshold value to provide for QoS differentiation. With the switch, each queue has 3 explicit programmable threshold classes—0, 1, 2. Therefore,

the enqueue/drop decision of each packet per queue is determined by the packet's threshold class assignment, which is determined by the DSCP, CoS, or QoS group field of the frame header.

WTD also uses a soft limit, and therefore you are allowed to configure the queue limit to up to 400 percent (maximum four times the reserved buffer from common pool). This soft limit prevents overrunning the common pool without impacting other features.

Note You can only configure queue limits on the switch egress queues on wired ports.

Before you begin

The following are prerequisites for this procedure:

- You should have created a class map for the queue limits before beginning this procedure.
- You must have configured either bandwidth, shape, or priority on the policy map prior to configuring the queue limits.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

Step 2	**policy-map** *policy name*
	Example:
	`Switch(config)# policy-map policy_queuelimit01`
	`Switch(config-pmap)#`
		Enters policy map configuration mode.
		Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

Step 3	**class** *class name*
	Example:
	`Switch(config-pmap)# class class_queuelimit01`
	`Switch(config-pmap-c)#`
		Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:
		• *word*—Class map name.
		• **class-default**—System default class matching any otherwise unclassified packets.

Step 4	**bandwidth** {*Kb/s* | **percent** *percentage* | **remaining** { **ratio** *ratio value* }} **Example:**	Configures the bandwidth for the policy map. The parameters include:

	Command or Action	Purpose
	`Switch(config-pmap-c)# bandwidth 500000` `Switch(config-pmap-c)#`	• *Kb/s*—Use this command to configure a specific value. The range is 20000 to 10000000. • **percent**—Allocates a minimum bandwidth to a particular class. The queue can oversubscribe bandwidth in case other queues do not utilize the entire port bandwidth. The total sum cannot exceed 100 percent, and in case it is less than 100 percent, the rest of the bandwidth is equally divided along all bandwidth queues. • **remaining**—Allocates a minimum bandwidth to a particular class. The queue can oversubscribe bandwidth in case other queues do not utilize entire port bandwidth. The total sum cannot exceed 100 percent. It is preferred to use this command when the **priority** command is used for certain queues in the policy. You can also assign ratios rather than a percentage to each queue; the queues will be assigned certain weights that are inline with these ratios. Ratios can range from 0 to 100. Total bandwidth ratio allocation for the policy in this case can exceed 100. **Note** You cannot mix bandwidth types on a policy map.

Step 5	**queue-limit** {*packets* **packets** | **cos** {*cos value* { *maximum threshold value* | **percent** *percentage* } | **values** {*cos value* | **percent** *percentage* } } | **dscp** {*dscp value* {*maximum threshold value* | **percent** *percentage*} | *match packet* {*maximum threshold value* | **percent** *percentage*} | **default** {*maximum threshold value* | **percent** *percentage*} | **ef** {*maximum threshold value* | **percent** *percentage*} | **dscp values** *dscp value*} | **percent** *percentage* }}
	Example:
	`Switch(config-pmap-c)# queue-limit dscp 3 percent 20`
	`Switch(config-pmap-c)# queue-limit dscp 4 percent 30`
	`Switch(config-pmap-c)# queue-limit dscp 5 percent 40`
		Sets the queue limit threshold percentage values.
		With every queue, there are three thresholds (0,1,2), and there are default values for each of these thresholds. Use this command to change the default or any other queue limit threshold setting. For example, if DSCP 3, 4, and 5 packets are being sent into a specific queue in a configuration, then you can use this command to set the threshold percentages for these three DSCP values. For additional information about queue limit threshold values, see Weighted Tail Drop, on page 618.
		Note The switch does not support absolute queue-limit percentages. The switch only supports DSCP or CoS queue-limit percentages.

	Command or Action	Purpose

Step 6	**end**
	Example:
	`Switch(config-pmap-c)# end`
	`Switch#`
		Saves configuration changes.

Step 7	**show policy-map** **Example:** `Switch# show policy-map`	(Optional) Displays policy configuration information for all classes configured for all service policies.

What to do next

Proceed to configure any additional policy maps for QoS for your network. After creating your policy maps, proceed to attach the traffic policy or polices to an interface using the **service-policy** command.

Related Topics

Weighted Tail Drop, on page 618
Examples: Queue-limit Configuration, on page 702

Configuring Shaping (CLI)

You use the **shape** command to configure shaping (maximum bandwidth) for a particular class. The queue's bandwidth is restricted to this value even though the port has additional bandwidth left. You can configure shaping as an average percent, as well as a shape average value in bits per second.

Before you begin

You should have created a class map for shaping before beginning this procedure.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

Step 2	**policy-map** *policy name*
	Example:
	`Switch(config)# policy-map policy_shaping01`
	`Switch(config-pmap)#`
		Enters policy map configuration mode.
		Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

	Command or Action	Purpose

Step 3	**class** *class name*
	Example:
	`Switch(config-pmap)# class class_shaping01`
	`Switch(config-pmap-c)#`
		Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:
		• *word*—Class map name.
		• **class-default**—System default class matching any otherwise unclassified packets.

Step 4	**shape average** {*target bit rate* | **percent** *percentage*}
	Example:
	`Switch(config-pmap-c)# shape average percent 50`
	`Switch(config-pmap-c)#`
		Configures the average shape rate. You can configure the average shape rate by target bit rates (bits per second) or by percentage of interface bandwidth for the Committed Information Rate (CIR).
		Note For the egress class-default SSID policy, you must configure the queue buffer ratio as 0 after you configure the average shape rate.

Step 5	**end**
	Example:
	`Switch(config-pmap-c)# end`
	`Switch#`
		Saves configuration changes.

Step 6	**show policy-map** **Example:** `Switch# show policy-map`	(Optional) Displays policy configuration information for all classes configured for all service policies.

What to do next

Configure any additional policy maps for QoS for your network. After creating your policy maps, attach the traffic policy or polices to an interface using the **service-policy** command.

Related Topics

Average Rate Shaping, on page 616
Examples: Average Rate Shaping Configuration, on page 701
Hierarchical Shaping, on page 616

Configuring Precious Metal Policies (CLI)

You can configure precious metal QoS policies on a per-WLAN basis.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 2	**wlan** *wlan-name* **Example:** `Switchwlan test4`	Enters the WLAN configuration submode.

Step 3	**service-policy** {**input** | **output**} *policy-name*
	Example:
	`Switch(config-wlan)# service-policy output platinum`
	Example:
	`Switch(config-wlan)# service-policy input platinum-up`
		Configures the WLAN with the QoS policy. To configure the WLAN with precious metal policies, you must enter one of the following keywords: **platinum**, **gold**, **silver**, or **bronze**. The upstream policy is specified with the keyword **platinum-up** as shown in the example.
		Note Upstream policies differ from downstream policies. The upstream policies have a suffix of -up.

Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit the global configuration mode.

Step 5	**show wlan** {*wlan-id* | *wlan-name*}
	Example:
	`Switch# show wlan name qos-wlan`
		Verifies the configured QoS policy on the WLAN.
		`Switch# show wlan name qos-wlan`
		`. . .`
		`. . .`
		`. . .`
		`QoS Service Policy - Input`
		`  Policy Name`
		`  : platinum-up`
		`  Policy State`
		`  : Validated`
		`QoS Service Policy - Output`
		`  Policy Name`
		`  : platinum`
		`  Policy State`
		`  : Validated`
		`. . .`
		`. . .`

Related Topics

Precious Metal Policies for Wireless QoS, on page 624

Configuring QoS Policies for Multicast Traffic (CLI)

Before you begin

The following are the prerequisites for configuring a QoS policy for multicast traffic:

- You must have a multicast service policy configured.
- You must enable multicast-multicast mode before applying the policy.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap capwap multicast service-policy output** *service-policy-name* **Example:** `Switch(config)#ap capwap multicast service-policy output service-policy-mcast`	Applies the configured multicast policy.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Wireless QoS Multicast, on page 610
Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic, on page 696

Configuring Port Policies (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless**

Step 2 Expand the **QoS** node by clicking on left pane and choose **QOS-Policy**.

The **QOS-Policy** page is displayed.

Step 3 Click **Add New** to create a new QoS policy.

The **Create QoS Policy** page is displayed.

Step 4 Select **Port** from the **Policy Type** drop-down menu.

Step 5 Enter the policy name in the **Policy Name** text field.

Step 6 Specify a description for the policy you want to create in the **Description** field.

Step 7 Configure the voice or video priorities for the port policies by enabling the Enable Voice and Enable Video parameters.

Note You must attach the port policy to an interface. Default values are recommended.

Step 8 Click **Add** to add the policy.

What to do next

Proceed to assign the port policy on an interface.

Related Topics

Port Policies, on page 596
Port Policy Format, on page 596
Restrictions for QoS on Wireless Targets, on page 632
Supported QoS Features on Wireless Targets, on page 594
Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic, on page 696

Applying or Changing Port Policies (GUI)

Procedure

Step 1 Choose **Configuration** > **Controller** > **System** > **Interfaces** > **Port Summary**.

The **Port Configuration** page is displayed.

Step 2 Select the interface on which you want to configure the port policy from the **Interface Name** column.

Step 3 Apply or change the **QoS Port Policy** by selecting the policy from the **Assign Policy** drop-down list.

The **Existing Policy** field displays the current policy assigned.

Note All interfaces in a channel group must be assigned to the same port policy.

Step 4 Click **Apply**.

Related Topics

Port Policies, on page 596
Port Policy Format, on page 596
Restrictions for QoS on Wireless Targets, on page 632
Supported QoS Features on Wireless Targets, on page 594
Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic, on page 696

Applying a QoS Policy on a WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless**.

Step 2 Expand the **WLAN** node by clicking on the left pane and choose **WLANs**.

The **WLANs** page is displayed.

Step 3 Select the WLAN for which you want to configure the QoS policies by clicking on the WLAN **Profile**.

Step 4 Click the QoS tab to configure the QoS policies on the WLAN.

You can also configure precious metal policies for the WLAN.

The following options are available:

Parameter	Description
QoS SSID Policy	
Egress Policy	QoS downstream policy configuration. The **Existing Policy** column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the **Assign Policy** column. If a policy is not selected, NONE is displayed.
Ingress Policy	QoS upstream policy configuration. The **Existing Policy** column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the **Assign Policy** column. If a policy is not selected, NONE is displayed.
QoS Client Policy	
Egress Policy	QoS downstream policy configuration. The **Existing Policy** column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the **Assign Policy** column. If a policy is not selected, NONE is displayed.
Ingress Policy	QoS upstream policy configuration. The **Existing Policy** column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the **Assign Policy** column. If a policy is not selected, NONE is displayed.
WMM	

Parameter	Description
WMM Policy	WMM Policy. This parameter has the following values: • Disabled—Disables this WMM policy. • Allowed—Allows the clients to communicate with the WLAN. • Require—Ensures that it is mandatory for the clients to have WMM features enabled on them to communicate with the WLAN.

Step 5 Click **Apply**.

Related Topics

Port Policies, on page 596
Port Policy Format, on page 596
Restrictions for QoS on Wireless Targets, on page 632
Supported QoS Features on Wireless Targets, on page 594
Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic, on page 696
SSID Policies, on page 598
Examples: SSID Policy
Examples: Configuring Downstream SSID Policy, on page 697
Client Policies, on page 599
Examples: Client Policies, on page 699

Monitoring QoS

The following commands can be used to monitor QoS on the switch.

Table 46: Monitoring QoS

Command	Description
show class-map [*class_map_name*]	Displays a list of all class maps configured.
show class-map type control subscriber {**all** | *name* } **show class-map type control subscriber detail**	Displays control class map and statistics. • all—Displays information for all class maps. • name—Displays configured class maps.

Command	Description
show policy-map [*policy_map_name*]	Displays a list of all policy maps configured. Command parameters include: • **policy map name** • **interface** • **session**

Command	Description
show policy-map interface { **Auto-template** | **Capwap** | **GigabitEthernet** | **GroupVI** | **InternalInterface** | **Lspvif** |**Loopback** | **Null** | **Port-channel** | **TenGigabitEthernet** | **Tunnel** | **Vlan** | **brief** | **class** | **input** | **output** | **wireless** }	Displays the runtime representation and statistics of all the policies configured on the switch. Command parameters include: • **Auto-template**—Auto-Template interface • **Capwap**—CAPWAP tunnel interface • **GigabitEthernet**—Gigabit Ethernet IEEE.802.3z • **GroupVI**—Group virtual interface • **InternalInterface**—Internal interface • **Loopback**—Loopback interface • **Null**—Null interface • **Lspvif**—LSP virtual interface • **Port-channel**—Ethernet channel of interfaces • **TenGigabitEthernet**—10-Gigabit Ethernet • **Tunnel**—Tunnel interface • **Vlan**—Catalyst VLANs • **brief**—Brief description of policy maps • **class**—Statistics for individual class • **input**—Input policy • **output**—Output policy • **wireless**—wireless
show policy-map interface wireless ap [*access point*]	Displays the runtime representation and statistics for all the wireless APs on the switch.
show policy-map interface wireless ssid [*ssid*]	Displays the runtime representation and statistics for all the SSID targets on the switch.

Command	Description
show policy-map interface wireless client mac [*mac_address*]	Displays the runtime representation and statistics for all the client targets on the switch.
show policy-map session [**input** | **output** | **uid** *UUID*]	Displays the session QoS policy. Command parameters include: • **input**—Input policy • **output**—Output policy • **uid**—Policy based on SSS unique identification.
show policy-map type control subscriber { **all** | **name** }	Displays the type QoS policy-map.
show table-map	Displays all the table maps and their configurations.
show platform qos wireless {**afd** { **client** | **ssid** } | **stats** { **bssid** *bssid-value* | **client** *name* | **ssid** {*ssid-value* | **all**} **client all**}}	Displays wireless targets. The following command parameters are supported: • afd—AFD information • stats—Statistics information
show policy-map interface wireless ssid name *ssid-name* [**radio type** {**24ghz** | **5ghz**} **ap name** *ap-name* | **ap name** *ap-name*]	Displays SSID policy configuration on an access point.
show wireless client mac-address *mac_address* **service-policy** {**input** | **output**}	Displays details of the client policy.
show wlan qos service-policies	Displays the SSID policies configured on all WLANs.
show ap name *ap_name* **service-policy**	Displays all the policies configured on the AP.

Monitoring SSID and Client Policies Statistics (GUI)

Statistics are supported only for ingress policies with a maximum of five classes on wireless targets. For very large policies, statistics for ingress policies are not visible at the switch. The frequency of the statistics depends on the number of clients associated with the access point.

Type of Statistics	Method	Details
SSID Policies	Choose **Monitor > Controller > Statistics > QoS**.	The QoS page is displayed with a list of SSID policies, Radio Type, and AP. Choose an SSID policy, radio, and access point from the drop-down lists and click **Apply** to view the statistics of the chosen SSID policy. You can view details such as match criteria, confirmed bytes, conformed rate, and exceeded rate.
Client Policies	Choose **Monitor > Clients > Client Details** .	The Clients page is displayed with a list of client MAC addresses, AP, and other details. Click the MAC address of a client and click the **QoS Statistics** tab. You can view details such as match criteria, confirmed bytes, conformed rate, and exceeded rate.

Configuration Examples for QoS

Examples: Classification by Access Control Lists

This example shows how to classify packets for QoS by using access control lists (ACLs):

```
Switch# configure terminal
Switch(config)# access-list 101 permit ip host 12.4.1.1 host 15.2.1.1
Switch(config)# class-map acl-101
Switch(config-cmap)# description match on access-list 101
Switch(config-cmap)# match access-group 101
Switch(config-cmap)#
```

After creating a class map by using an ACL, you then create a policy map for the class, and apply the policy map to an interface for QoS.

Related Topics

Creating a Traffic Class (CLI), on page 635
Class Maps, on page 608

Examples: Class of Service Layer 2 Classification

This example shows how to classify packets for QoS using a class of service Layer 2 classification:

```
Switch# configure terminal
Switch(config)# class-map cos
Switch(config-cmap)# match cos ?
  <0-7>  Enter up to 4 class-of-service values separated by white-spaces
Switch(config-cmap)# match cos 3 4 5
Switch(config-cmap)#
```

After creating a class map by using a CoS Layer 2 classification, you then create a policy map for the class, and apply the policy map to an interface for QoS.

Examples: Class of Service DSCP Classification

This example shows how to classify packets for QoS using a class of service DSCP classification:

```
Switch# configure terminal
Switch(config)# class-map dscp
Switch(config-cmap)# match dscp af21 af22 af23
Switch(config-cmap)#
```

After creating a class map by using a DSCP classification, you then create a policy map for the class, and apply the policy map to an interface for QoS.

Examples: VLAN ID Layer 2 Classification

This example shows how to classify for QoS using a VLAN ID Layer 2 classification:

```
Switch# configure terminal
Switch(config)# class-map vlan-120
Switch(config-cmap)# match vlan ?
  <1-4095>  VLAN id
Switch(config-cmap)# match vlan 120
Switch(config-cmap)#
```

After creating a class map by using a VLAN Layer 2 classification, you then create a policy map for the class, and apply the policy map to an interface for QoS.

Examples: Classification by DSCP or Precedence Values

This example shows how to classify packets by using DSCP or precedence values:

```
Switch# configure terminal
Switch(config)# class-map prec2
Switch(config-cmap)# description matching precedence 2 packets
Switch(config-cmap)# match ip precedence 2
Switch(config-cmap)# exit
Switch(config)# class-map ef
Switch(config-cmap)# description EF traffic
Switch(config-cmap)# match ip dscp ef
Switch(config-cmap)#
```

After creating a class map by using a DSCP or precedence values, you then create a policy map for the class, and apply the policy map to an interface for QoS.

Examples: Hierarchical Classification

The following is an example of a hierarchical classification, where a class named parent is created, which matches another class named child. The class named child matches based on the IP precedence being set to 2.

```
Switch# configure terminal
Switch(config)# class-map child
Switch(config-cmap)# match ip precedence 2
Switch(config-cmap)# exit
Switch(config)# class-map parent
Switch(config-cmap)# match class child
Switch(config-cmap)#
```

After creating the parent class map, you then create a policy map for the class, and apply the policy map to an interface for QoS.

Related Topics

Hierarchical QoS, on page 600

Examples: Hierarchical Policy Configuration

The following is an example of a configuration using hierarchical polices:

```
Switch# configure terminal
Switch(config)# class-map c1
Switch(config-cmap)# match dscp 30
Switch(config-cmap)# exit

Switch(config)# class-map c2
Switch(config-cmap)# match precedence 4
Switch(config-cmap)# exit

Switch(config)# class-map c3
Switch(config-cmap)# exit

Switch(config)# policy-map child
Switch(config-pmap)# class c1
Switch(config-pmap-c)# priority level 1
Switch(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit

Switch(config-pmap)# class c2
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit

Switch(config)# policy-map parent
Switch(config-pmap)# class class-default
```

```
Switch(config-pmap-c)# shape average 1000000
Switch(config-pmap-c)# service-policy child
Switch(config-pmap-c)# end
```

The following example shows a hierarchical policy using table maps:

```
Switch(config)# table-map dscp2dscp
 Switch(config-tablemap)# default copy
Switch(config)# table-map dscp2up
Switch(config-tablemap)# map from 46 to 6
Switch(config-tablemap)# map from 34 to 5
Switch(config-tablemap)# default copy
Switch(config)# policy-map ssid_child_policy
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority level 1
Switch(config-pmap-c)# police 15000000
Switch(config-pmap)# class video
Switch(config-pmap-c)# priority level 2
Switch(config-pmap-c)# police 10000000
Switch(config)# policy-map ssid_policy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 30000000
Switch(config-pmap-c)# queue-buffer ratio 0
Switch(config-pmap-c)# set dscp dscp table dscp2dscp
Switch(config-pmap-c)# service-policy ssid_child_policy
```

Related Topics

Hierarchical QoS, on page 600

Examples: Classification for Voice and Video

This example describes how to classify packet streams for voice and video using switch specific information.

In this example, voice and video are coming in from end-point A into GigabitEthernet1/0/1 on the switch and have precedence values of 5 and 6, respectively. Additionally, voice and video are also coming from end-point B into GigabitEthernet1/0/2 on the switch with DSCP values of EF and AF11, respectively.

Assume that all the packets from the both the interfaces are sent on the uplink interface, and there is a requirement to police voice to 100 Mbps and video to 150 Mbps.

To classify per the above requirements, a class to match voice packets coming in on GigabitEthernet1/0/1 is created, named voice-interface-1, which matches precedence 5. Similarly another class for voice is created, named voice-interface-2, which will match voice packets in GigabitEthernet1/0/2. These classes are associated to two separate policies named input-interface-1, which is attached to GigabitEthernet1/0/1, and input-interface-2, which is attached to GigabitEthernet1/0/2. The action for this class is to mark the qos-group to 10. To match packets with QoS-group 10 on the output interface, a class named voice is created which matches on QoS-group 10. This is then associated to another policy named output-interface, which is associated to the uplink interface. Video is handled in the same way, but matches on QoS-group 20.

The following example shows how classify using the above switch specific information:

```
Switch(config)#
Switch(config)# class-map voice-interface-1
Switch(config-cmap)# match ip precedence 5
Switch(config-cmap)# exit

Switch(config)# class-map video-interface-1
Switch(config-cmap)# match ip precedence 6
```

```
Switch(config-cmap)# exit

Switch(config)# class-map voice-interface-2
Switch(config-cmap)# match ip dscp ef
Switch(config-cmap)# exit

Switch(config)# class-map video-interface-2
Switch(config-cmap)# match ip dscp af11
Switch(config-cmap)# exit

Switch(config)# policy-map input-interface-1
Switch(config-pmap)# class voice-interface-1
Switch(config-pmap-c)# set qos-group 10
Switch(config-pmap-c)# exit

Switch(config-pmap)# class video-interface-1
Switch(config-pmap-c)# set qos-group 20

Switch(config-pmap-c)# policy-map input-interface-2
Switch(config-pmap)# class voice-interface-2
Switch(config-pmap-c)# set qos-group 10
Switch(config-pmap-c)# class video-interface-2
Switch(config-pmap-c)# set qos-group 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit

Switch(config)# class-map voice
Switch(config-cmap)# match qos-group 10
Switch(config-cmap)# exit

Switch(config)# class-map video
Switch(config-cmap)# match qos-group 20

Switch(config)# policy-map output-interface
Switch(config-pmap)# class voice
Switch(config-pmap-c)# police 256000 conform-action transmit exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit

Switch(config-pmap)# class video
Switch(config-pmap-c)# police 1024000 conform-action transmit exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
```

Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic

The following example provides a template for creating a port child policy for managing quality of service for voice and video traffic.

```
Policy-map port_child_policy
    Class voice (match dscp ef)
            Priority level 1
            Police  Multicast Policer
    Class video (match dscp af41)
            Priority level 2
            Police  Multicast Policer
    Class mcast-data  (match non-client-nrt)
```

```
        Bandwidth remaining ratio <>
Class class-default   (NRT Data)
        Bandwidth remaining ratio <>
```

Note Multicast Policer in the example above is not a keyword. It refers to the policing policy configured.

Two class maps with name voice and video are configured with DSCP assignments of 46 and 34. The voice traffic is assigned the priority of 1 and the video traffic is assigned the priority level 2 and is processed using Q0 and Q1. If your network receives multicast voice and video traffic, you can configure multicast policers. The non-client NRT data and NRT data are processed using the Q2 and Q3 queues.

Related Topics

Configuring Port Policies (GUI), on page 685
Applying or Changing Port Policies (GUI), on page 686
Applying a QoS Policy on a WLAN (GUI), on page 687
Port Policies, on page 596
Port Policy Format, on page 596
Configuring QoS Policies for Multicast Traffic (CLI), on page 685
Wireless QoS Multicast, on page 610

Examples: Configuring Downstream SSID Policy

To configure a downstream BSSID policy, you must first configure a port child policy with priority level queuing.

Type of Policy	Example

User-defined port child policy	`policy-map port_child_policy`
	`  class voice`
	`  priority level 1 20000`
	
	`  class video`
	`  priority level 2 10000`
	
	`  class non-client-nrt-class`
	`  bandwidth remaining ratio 10`
	
	`  class class-default`
	`  bandwidth remaining ratio 15`

Egress BSSID policy	`policy-map bssid-policer`
	`  queue-buffer ratio 0`
	`  class class-default`
	`  shape average 30000000`
	`set dscp dscp table dscp2dscp`
	`set wlan user-priority dscp table dscp2up`
	`service-policy ssid_child_qos`

Type of Policy	Example
SSID Child QoS policy	Policy Map ssid-child_qos Class voice priority level 1 police cir 5m admit cac wmm-tspec UP 6,7 / tells WCM allow 'voice' TSPEC\SIP snoop for this ssid rate 4000 / must be police rate value is in kbps) Class video priority level 2 police cir 60000

Related Topics

Applying an SSID or Client Policy on a WLAN (CLI), on page 653
Configuring SSID Policies (GUI), on page 652
Applying a QoS Policy on a WLAN (GUI), on page 687
SSID Policies, on page 598

Examples: Ingress SSID Policies

The following examples show ingress SSID hierarchical policies:

Type of ingress SSID policies	Example
Ingress SSID hierarchical policies	policy-map ssid-child-policy class voice //match dscp 46 police 3m class video //match dscp 34 police 4m policy-map ssid-in-policy class class-default set dscp wlan user-priority table up2dscp service-policy ssid-child-policy
	policy-map ssid_in_policy class dscp-40 set cos 1 police 10m class up-1 set dscp 34 police 12m class dscp-10 set dscp 20 police 15m class class-default set dscp wlan user-priority table up2dscp police 50m

Examples: Client Policies

Type of Client Policy	Example/Details

Default egress client policy	Any incoming traffic contains the user-priority as 0.
	Note The default client policy is enabled only on WMM clients that are ACM-enabled.
	You can verify if ACM is enabled by using the **show ap dot11 5ghz network** command. To enable ACM, use the **ap dot11 5ghz cac voice acm** command.
	`Policy-map client-def-down`
	`  class class-default`
	`      set wlan user-priority 0`

Default ingress client policy	Any traffic that is sent to the wired network from wireless network will result in the DSCP value being set to 0.
	Note The default client policy is enabled only on WMM clients that are ACM-enabled.
	`Policy-map client-def-up`
	`   class class-default`
	`    set dscp 0`

Client policies generated automatically and applied to the WMM client when the client authenticates to a profile in AAA with a configured QoS-level attribute.	`Policy Map platinum-WMM`
	`Class voice-plat`
	`  set wlan user-priority 6`
	` Class video-plat`
	` set wlan user-priority 4`
	`Class class-default`
	`  set wlan user-priority 0`
	`Policy Map gold-WMM`
	`Class voice-gold`
	`  set wlan user-priority 4`
	` Class video-gold`
	` set wlan user-priority 4`
	`Class class-default`
	`  set wlan user-priority 0`

Non-WMM client precious metal policies	`Policy Map platinum` `  set wlan user-priority 6`

Type of Client Policy	Example/Details

Egress client policy where any traffic matching class voice1, the user priority is set to a pre-defined value.	The class can be set to assign a DSCP or ACL.
	
	`Policy Map client1-down`
	`Class voice1 //match dscp, cos`
	`set wlan user-priority <>`
	`Class voice2 //match acl`
	`set wlan user-priority <>`
	`Class voice3`
	`set wlan user-priority <>`
	`Class class-default`
	`set wlan user-priority 0`

Client policy based on AAA and TCLAS	`Policy Map client2-down[ AAA+ TCLAS pol example]`
	`Class voice\\match dscp`
	`police <>`
	`set <>`
	`Class class-default`
	`set <>`
	`Class voice1|| voice2 [match acls]`
	`police <>`
	`class voice1`
	`set <>`
	`class voice2`
	`set <>`

Client policy for voice and video for traffic in the egress direction	`Policy Map client3-down`
	`class voice \\match dscp, cos`
	`police X`
	`class video`
	`police Y`
	`class class-default`
	`police Z`

Client policy for voice and video for traffic in the ingress direction using policing	`Policy Map client1-up`
	`class voice \\match dscp, up, cos`
	`police X`
	`class video`
	`police Y`
	`class class-default`
	`police Z`

Client policy for voice and video based on DSCP	`Policy Map client2-up`
	`class voice \\match dscp, up, cos`
	`set dscp <>`
	`class video`
	`set dscp <>`
	`class class-default`
	`set dscp <>`

Type of Client Policy	Example/Details
Client ingress policy with marking and policing	policy-map client_in_policy class dscp-48 //match dscp 48 set cos 3 police 2m class up-4 //match wlan user-priority 4 set dscp 10 police 3m class acl //match acl set cos 2 police 5m class class-default set dscp 20 police 15m
Hierarchical client ingress policy	policy-map client-child-policy class voice //match dscp 46 set dscp 40 police 5m class video //match dscp 34 set dscp 30 police 7m policy-map client-in-policy class class-default police 15m service-policy client-child-policy

Related Topics

Configuring Client Policies (CLI)
Configuring Client Policies (GUI), on page 642
Applying a QoS Policy on a WLAN (GUI), on page 687
Client Policies, on page 599

Examples: Average Rate Shaping Configuration

The following example shows how to configure average rate shaping:

```
Switch# configure terminal
Switch(config)# class-map prec1
Switch(config-cmap)# description matching precedence 1 packets
Switch(config-cmap)# match ip precedence 1
Switch(config-cmap)# end

Switch# configure terminal
Switch(config)# class-map prec2
Switch(config-cmap)# description matching precedence 2 packets
Switch(config-cmap)# match ip precedence 2
Switch(config-cmap)# exit

Switch(config)# policy-map shaper
Switch(config-pmap)# class prec1
Switch(config-pmap-c)# shape average 512000
Switch(config-pmap-c)# exit
```

```
Switch(config-pmap)# policy-map shaper
Switch(config-pmap)# class prec2
Switch(config-pmap-c)# shape average 512000
Switch(config-pmap-c)# exit

Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 1024000
```

After configuring the class maps, policy map, and shape averages for your configuration, proceed to then apply the policy map to the interface for QoS.

Related Topics

Configuring Shaping (CLI), on page 682
Average Rate Shaping, on page 616

Examples: Queue-limit Configuration

The following example shows how to configure a queue-limit policy based upon DSCP values and percentages:

```
Switch# configure terminal
Switch#(config)# policy-map port-queue
Switch#(config-pmap)# class dscp-1-2-3
Switch#(config-pmap-c)# bandwidth percent 20
Switch#(config-pmap-c)# queue-limit dscp 1 percent 80
Switch#(config-pmap-c)# queue-limit dscp 2 percent 90
Switch#(config-pmap-c)# queue-limit dscp 3 percent 100
Switch#(config-pmap-c)# exit

Switch#(config-pmap)# class dscp-4-5-6
Switch#(config-pmap-c)# bandwidth percent 20
Switch#(config-pmap-c)# queue-limit dscp 4 percent 20
Switch#(config-pmap-c)# queue-limit dscp 5 percent 30
Switch#(config-pmap-c)# queue-limit dscp 6 percent 20
Switch#(config-pmap-c)# exit

Switch#(config-pmap)# class dscp-7-8-9
Switch#(config-pmap-c)# bandwidth percent 20
Switch#(config-pmap-c)# queue-limit dscp 7 percent 20
Switch#(config-pmap-c)# queue-limit dscp 8 percent 30
Switch#(config-pmap-c)# queue-limit dscp 9 percent 20
Switch#(config-pmap-c)# exit

Switch#(config-pmap)# class dscp-10-11-12
Switch#(config-pmap-c)# bandwidth percent 20
Switch#(config-pmap-c)# queue-limit dscp 10 percent 20
Switch#(config-pmap-c)# queue-limit dscp 11 percent 30
Switch#(config-pmap-c)# queue-limit dscp 12 percent 20
Switch#(config-pmap-c)# exit

Switch#(config-pmap)# class dscp-13-14-15
Switch#(config-pmap-c)# bandwidth percent 10
Switch#(config-pmap-c)# queue-limit dscp 13 percent 20
Switch#(config-pmap-c)# queue-limit dscp 14 percent 30
Switch#(config-pmap-c)# queue-limit dscp 15 percent 20
Switch#(config-pmap-c)# end
Switch#
```

After finishing with the above policy map queue-limit configuration, you can then proceed to apply the policy map to an interface for QoS.

Related Topics

Configuring Queue Limits (CLI), on page 679
Weighted Tail Drop, on page 618

Examples: Queue Buffers Configuration

The following example shows how configure a queue buffer policy and then apply it to an interface for QoS:

```
Switch# configure terminal
Switch(config)# policy-map policy1001
Switch(config-pmap)# class class1001
Switch(config-pmap-c)# bandwidth remaining ratio 10
Switch(config-pmap-c)# queue-buffer ratio ?
  <0-100>  Queue-buffers ratio limit
Switch(config-pmap-c)# queue-buffer ratio 20
Switch(config-pmap-c)# end

Switch# configure terminal
Switch(config)# interface gigabitEthernet2/0/3
Switch(config-if)# service-policy output policy1001
Switch(config-if)# end
```

Related Topics

Configuring Queue Buffers (CLI), on page 677
Queue Buffer Allocation, on page 620

Examples: Policing Action Configuration

The following example displays the various policing actions that can be associated to the policer. These actions are accomplished using the conforming, exceeding, or violating packet configurations. You have the flexibility to drop, mark and transmit, or transmit packets that have exceeded or violated a traffic profile.

For example, a common deployment scenario is one where the enterprise customer polices traffic exiting the network towards the service provider and marks the conforming, exceeding and violating packets with different DSCP values. The service provider could then choose to drop the packets marked with the exceeded and violated DSCP values under cases of congestion, but may choose to transmit them when bandwidth is available.

Note The Layer 2 fields can be marked to include the CoS fields, and the Layer 3 fields can be marked to include the precedence and the DSCP fields.

One useful feature is the ability to associate multiple actions with an event. For example, you could set the precedence bit and the CoS for all conforming packets. A submode for an action configuration could then be provided by the policing feature.

This is an example of a policing action configuration:

```
Switch# configure terminal
```

```
Switch(config)# policy-map police
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# police cir 1000000 pir 2000000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit dscp table exceed-markdown-table
Switch(config-pmap-c-police)# violate-action set-dscp-transmit dscp table
violate-markdown-table
Switch(config-pmap-c-police)# end
```

In this example, the exceed-markdown-table and violate-mark-down-table are table maps.

Note Policer-based markdown actions are only supported using table maps. Only one markdown table map is allowed for each marking field in the switch.

Related Topics

Configuring Police (CLI), on page 672
Policing, on page 610
Token-Bucket Algorithm, on page 611

Examples: Policer VLAN Configuration

The following example displays a VLAN policer configuration. At the end of this configuration, the VLAN policy map is applied to an interface for QoS.

```
Switch# configure terminal
Switch(config)# class-map vlan100
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# exit
Switch(config)# policy-map vlan100
Switch(config-pmap)# policy-map class vlan100
Switch(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
Switch(config-pmap-c-police)# end
Switch# configure terminal
Switch(config)# interface gigabitEthernet1/0/5
Switch(config-if)#  service-policy input vlan100
```

Related Topics

Classifying, Policing, and Marking Traffic on SVIs by Using Policy Maps (CLI), on page 657
Policy Map on VLANs, on page 609

Examples: Policing Units

The following examples display the various units of policing that are supported for QoS. The policing unit is the basis on which the token bucket works .

The following units of policing are supported:

- CIR and PIR are specified in bits per second. The burst parameters are specified in bytes. This is the default mode; it is the unit that is assumed when no units are specified. The CIR and PIR can also be configured in percent, in which case the burst parameters have to be configured in milliseconds.

- CIR and PIR are specified in packets per second. In this case, the burst parameters are configured in packets as well.

The following is an example of a policer configuration in bits per second:

```
Switch(config)# policy-map bps-policer
Switch(config-pmap)# class class-default
Switch(config-pmap-c) # police rate 256000 bps burst 1000 bytes
conform-action transmit exceed-action drop
```

The following is an example of a policer configuration in packets per second. In this configuration, a dual-rate three-color policer is configured where the units of measurement is packet. The burst and peak burst are all specified in packets.

```
Switch(config)# policy-map pps-policer
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# police rate 5000 pps burst 100 packets
peak-rate 10000 pps peak-burst 200 packets conform-action transmit
exceed-action drop violate-action drop
```

Related Topics

Configuring Police (CLI), on page 672
Token-Bucket Algorithm, on page 611

Examples: Single-Rate Two-Color Policing Configuration

The following example shows how to configure a single-rate two-color policer:

```
Switch(config)# class-map match-any prec1
Switch(config-cmap)# match ip precedence 1
Switch(config-cmap)# exit
Switch(config)# policy-map policer
Switch(config-pmap)# class prec1
Switch(config-pmap-c)# police cir 256000 conform-action transmit exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)#
```

Related Topics

Configuring Police (CLI), on page 672
Single-Rate Two-Color Policing, on page 614

Examples: Dual-Rate Three-Color Policing Configuration

The following example shows how to configure a dual-rate three-color policer:

```
Switch# configure terminal
Switch(config)# policy-Map dual-rate-3color-policer
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# police cir 64000 bc 2000 pir 128000 be 2000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit dscp table exceed-markdown-table
Switch(config-pmap-c-police)# violate-action set-dscp-transmit dscp table
```

```
violate-markdown-table
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)#
```

In this example, the exceed-markdown-table and violate-mark-down-table are table maps.

Note Policer based markdown actions are only supported using table maps. Only one markdown table map is allowed for each marking field in the switch.

Related Topics

Configuring Police (CLI), on page 672
Dual-Rate Three-Color Policing, on page 615

Examples: Table Map Marking Configuration

The following steps and examples show how to use table map marking for your QoS configuration:

1. Define the table map.

   Define the table-map using the **table-map** command and indicate the mapping of the values. This table does not know of the policies or classes within which it will be used. The default command in the table map indicates the value to be copied into the 'to' field when there is no matching 'from' field. In the example, a table map named table-map1 is created. The mapping defined is to convert the value from 0 to 1 and from 2 to 3, while setting the default value to 4.

   ```
   Switch(config)# table-map table-map1
   Switch(config-tablemap)# map from 0 to 1
   Switch(config-tablemap)# map from 2 to 3
   Switch(config-tablemap)# default 4
   Switch(config-tablemap)# exit
   ```

2. Define the policy map where the table map will be used.

   In the example, the incoming CoS is mapped to the DSCP based on the mapping specified in the table table-map1. For this example, if the incoming packet has a DSCP of 0, the CoS in the packet is set 1. If no table map name is specified the command assumes a default behavior where the value is copied as is from the 'from' field (DSCP in this case) to the 'to' field (CoS in this case). Note however, that while the CoS is a 3-bit field, the DSCP is a 6-bit field, which implies that the CoS is copied to the first three bits in the DSCP.

   ```
   Switch(config)# policy map policy1
   Switch(config-pmap)# class class-default
   Switch(config-pmap-c)# set cos dscp table table-map1
   Switch(config-pmap-c)# exit
   ```

3. Associate the policy to an interface.

   ```
   Switch(config)# interface GigabitEthernet1/0/1
   Switch(config-if)# service-policy output policy1
   ```

```
Switch(config-if)# exit
```

Related Topics

Configuring Table Maps (CLI), on page 660
Table Map Marking, on page 612

Example: Table Map Configuration to Retain CoS Markings

The following example shows how to use table maps to retain CoS markings on an interface for your QoS configuration.

The cos-trust-policy policy (configured in the example) is enabled in the ingress direction to retain the CoS marking coming into the interface. If the policy is not enabled, only the DSCP is trusted by default. If a pure Layer 2 packet arrives at the interface, then the CoS value will be rewritten to 0 when there is no such policy in the ingress port for CoS.

```
Switch# configure terminal
Switch(config)# table-map cos2cos
Switch(config-tablemap)# default copy
Switch(config-tablemap)# exit


Switch(config)# policy map cos-trust-policy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set cos cos table cos2cos
Switch(config-pmap-c)# exit

Switch(config)# interface GigabitEthernet1/0/2
Switch(config-if)# service-policy input cos-trust-policy
Switch(config-if)# exit
```

Related Topics

Trust Behavior for Wired and Wireless Ports, on page 621

Additional References for QoS

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	*QoS Command Reference (Catalyst 3850 Switches)QoS Command Reference (Cisco WLC 5700 Series)* *Cisco IOS Quality of Service Solutions Command Reference*

Related Topic	Document Title
Call Admission Control (CAC)	*System Management Configuration Guide (Catalyst 3850 Switches)System Management Configuration Guide (Cisco WLC 5700 Series)* *System Management Command Reference (Catalyst 3850 Switches)System Management Command Reference (Cisco WLC 5700 Series)*
Multicast Shaping and Policing Rate	*IP Multicast Routing Configuration Guide (Catalyst 3850 Switches)Routing Configuration Guide (Cisco WLC 5700 Series)*
Application Visibility and Control	*System Management Configuration Guide (Catalyst 3850 Switches)System Management Configuration Guide (Cisco WLC 5700 Series)* *System Management Command Reference (Catalyst 3850 Switches)System Management Command Reference (Cisco WLC 5700 Series)*
Application Visibility and Control	*System Management Configuration Guide (Catalyst 3850 Switches)System Management Configuration Guide (Cisco WLC 5700 Series)* *System Management Command Reference (Catalyst 3850 Switches)System Management Command Reference (Cisco WLC 5700 Series)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
—	

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

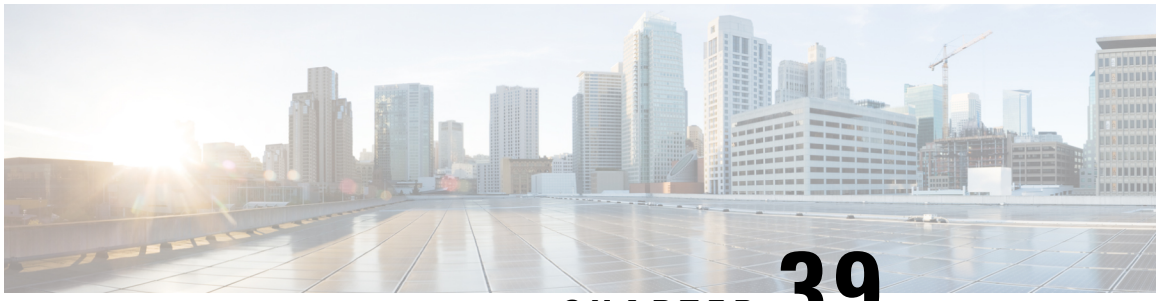
Feature History and Information for QoS

Release	Modification
Cisco IOS XE 3.3SE	This feature was introduced.
Cisco IOS XE 3.3SE	Consistent system default trust behavior for both wired and wireless ports. The Cisco IOS XE 3.2 Release supported different trust defaults for wired and wireless ports. The trust default for wired ports was the same as for this software release. For wireless ports, the default system behavior was non-trust, which meant that when the switch came up, all markings for the wireless ports were defaulted to zero and no traffic received priority treatment. For compatibility with an existing wired switch, all traffic went to the best-effort queue by default. The access point performed priority queuing by default. The default trust behavior in the case of wireless ports could be changed by using the **no qos wireless default untrust** command.

Release	Modification
Cisco IOS XE 3.3SE	Support for IPv6 wireless clients. The Cisco IOS XE 3.2 software release did not support IPv6 for wireless clients. This is now supported. Client policies can now have IPv4 and IPv6 filters.
Cisco IOS XE 3.3SE	Support for 3 radios and 11ac.
Cisco IOS XE 3.3SE	New classification counters available in the **show policy-map** command. **Note** This feature is only available on wired targets.
Cisco IOS XE 3.6E	Marking and policing actions for ingress SSID policies. Client policies are applied at the access point.
Cisco IOS XE 3.6E	New classification counters for wireless targets available in the **show policy-map** command.
Cisco IOS XE 3.6E	Statistics are supported only for ingress policies.

PART X

Radio Resource Management



CHAPTER 39

Configuring Radio Resource Management

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Radio Resource Management

The switch should be configured as a mobility controller and not a mobility anchor to configure Radio Resource Management. It may require dynamic channel assignment functionality for the home APs to be supported.

The new mobility architecture that involves mobility controller and mobility agent must be configured on the switch or controllers for RRM to work.

Note Refer Mobility Configuration Guide for configuring mobility controller and mobility agent.

Restrictions for Radio Resource Management

The number of APs in a RF-group is limited to 2000.

The number of APs in a RF-group is limited to 500.

If an AP tries to join the RF-group that already holds the maximum number of APs it can support, the device rejects the application and throws an error.

To enable Airtime Fairness mode for APs, you should disable enforce-policy mode and reapply it again. This will change the airtime fairness configuration for all the APs. You can also use the **ap name <ap-name> dot11 24ghz airtime-fairness mode enforce-policy** command to change airtime fairness mode for individual APs.

Information About Radio Resource Management

The Radio Resource Management (RRM) software embedded in the switch acts as a built-in RF engineer to consistently provide real-time RF management of your wireless network. RRM enables switches to continually monitor their associated lightweight access points for the following information:

- Traffic load—The total bandwidth used for transmitting and receiving traffic. It enables wireless LAN managers to track and plan network growth ahead of client demand.
- Interference—The amount of traffic coming from other 802.11 sources.
- Noise—The amount of non-802.11 traffic that is interfering with the currently assigned channel.
- Coverage—The Received Signal Strength (RSSI) and signal-to-noise ratio (SNR) for all connected clients.
- Other —The number of nearby access points.

RRM performs these functions:

- Radio resource monitoring
- Transmit power control
- Dynamic channel assignment
- Coverage hole detection and correction
- RF grouping

Note RRM grouping will not happen, since AP operates in a static channel which is not in the DCA channel list. NDP is sent only on DCA channels and when radio operates on a non-DCA channel it will not receive NDA on-channel.

Radio Resource Monitoring

RRM automatically detects and configures new switches and lightweight access points as they are added to the network. It then automatically adjusts associated and nearby lightweight access points to optimize coverage and capacity.

Lightweight access points can scan all valid 2.4 GHz and 5 GHz channels for the country of operation as well as for channels available in other locations. The access points in local mode go "off-channel" for a period not greater than 60 ms to monitor these channels for noise and interference. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and interfering access points.

Note In the presence of voice traffic or other critical traffic (in the last 100 ms), the access points can defer off-channel measurements. It also defers based on WLAN scan defer priority configurations.

Each access point spends only 0.2 percent of its time off-channel. This activity is distributed across all access points so that adjacent access points are not scanning at the same time, which could adversely affect wireless LAN performance.

RRM supports new mobility architecture for RF grouping that involves Mobility Controller (MC) and Mobility Agent (MA).

- Mobility Controller (MC)—The Cisco WLC 5700 Series Controllers, Cisco Catalyst 3850 Switch, or Cisco Unified Wireless Networking Solution controller can act as MC. The MC has MC functionality and MA functionality that is running internally into it.
- Mobility Agent (MA)—The Mobility Agent is the component that maintains client mobility state machine for a mobile client.

Information About RF Groups

An RF group is a logical collection of Cisco WLCs that coordinate to perform RRM in a globally optimized manner to perform network calculations on a per-radio basis. An RF group exists for each 802.11 network type. Clustering Cisco WLCs into a single RF group enables the RRM algorithms to scale beyond the capabilities of a single Cisco WLC.

RF group is created based on the following parameters:

- User-configured RF network name.
- Neighbor discovery performed at the radio level.
- Country list configured on MC.

RF grouping runs between MCs.

Lightweight access points periodically send out neighbor messages over the air. Access points using the the same RF group name validate messages from each other.

When access points on different Cisco WLCs hear validated neighbor messages at a signal strength of –80 dBm or stronger, the Cisco WLCs dynamically form an RF neighborhood in auto mode. In static mode, the leader is manually selected and the members are added to the RF Group. .

Note RF groups and mobility groups are similar in that they both define clusters of Cisco WLCs, but they are different in terms of their use. An RF group facilitates scalable, system-wide dynamic RF management while a mobility group facilitates scalable, system-wide mobility and Cisco WLC redundancy.

RF Group Leader

Starting in the 7.0.116.0 release, the RF Group Leader can be configured in two ways as follows:

- Auto Mode—In this mode, the members of an RF group elect an RF group leader to maintain a "master" power and channel scheme for the group. The RF grouping algorithm dynamically chooses the RF group leader and ensures that an RF group leader is always present. Group leader assignments can and do change (for instance, if the current RF group leader becomes inoperable or RF group members experience major changes).
- Static Mode—In this mode, the user selects a Cisco WLC as an RF group leader manually. In this mode, the leader and the members are manually configured and fixed. If the members are unable to join the RF group, the reason is indicated. The leader tries to establish a connection with a member every one minute if the member has not joined in the previous attempt.

The RF group leader analyzes real-time radio data collected by the system, calculates the power and channel assignments, and sends them to each of the Cisco WLCs in the RF group. The RRM algorithms ensure system-wide stability, and restrain channel and power scheme changes to the appropriate local RF neighborhoods.

In Cisco WLC software releases prior to 6.0, the dynamic channel assignment (DCA) search algorithm attempts to find a good channel plan for the radios associated to Cisco WLCs in the RF group, but it does not adopt a new channel plan unless it is considerably better than the current plan. The channel metric of the worst radio in both plans determines which plan is adopted. Using the worst-performing radio as the single criterion for adopting a new channel plan can result in pinning or cascading problems.

Pinning occurs when the algorithm could find a better channel plan for some of the radios in an RF group but is prevented from pursuing such a channel plan change because the worst radio in the network does not have any better channel options. The worst radio in the RF group could potentially prevent other radios in the group from seeking better channel plans. The larger the network, the more likely pinning becomes.

Cascading occurs when one radio's channel change results in successive channel changes to optimize the remaining radios in the RF neighborhood. Optimizing these radios could lead to their neighbors and their neighbors' neighbors having a suboptimal channel plan and triggering their channel optimization. This effect could propagate across multiple floors or even multiple buildings, if all the access point radios belong to the same RF group. This change results in considerable client confusion and network instability.

The main cause of both pinning and cascading is the way in which the search for a new channel plan is performed and that any potential channel plan changes are controlled by the RF circumstances of a single radio. In Cisco WLC software release 6.0, the DCA algorithm has been redesigned to prevent both pinning and cascading. The following changes have been implemented:

- Multiple local searches—The DCA search algorithm performs multiple local searches initiated by different radios in the same DCA run rather than performing a single global search driven by a single radio. This change addresses both pinning and cascading while maintaining the desired flexibility and adaptability of DCA and without jeopardizing stability.

- Multiple Channel Plan Change Initiators (CPCIs)—Previously, the single worst radio was the sole initiator of a channel plan change. Now each radio in the RF group is evaluated and prioritized as a potential initiator. Intelligent randomization of the resulting list ensures that every radio is eventually evaluated, which eliminates the potential for pinning.
- Limiting the propagation of channel plan changes (Localization)—For each CPCI radio, the DCA algorithm performs a local search for a better channel plan, but only the CPCI radio itself and its one-hop neighboring access points are actually allowed to change their current transmit channels. The impact of an access point triggering a channel plan change is felt only to within two RF hops from that access point, and the actual channel plan changes are confined to within a one-hop RF neighborhood. Because this limitation applies across all CPCI radios, cascading cannot occur.
- Non-RSSI-based cumulative cost metric—A cumulative cost metric measures how well an entire region, neighborhood, or network performs with respect to a given channel plan. The individual cost metrics of all access points in that area are considered in order to provide an overall understanding of the channel plan's quality. These metrics ensure that the improvement or deterioration of each single radio is factored into any channel plan change. The objective is to prevent channel plan changes in which a single radio improves but at the expense of multiple other radios experiencing a considerable performance decline.

The RRM algorithms run at a specified updated interval, which is 600 seconds by default. Between update intervals, the RF group leader sends keepalive messages to each of the RF group members and collects real-time RF data.

Note Several monitoring intervals are also available. See the Configuring RRM section for details.

RF Group Name

A Cisco WLC is configured in an RF group name, which is sent to all access points joined to the Cisco WLC and used by the access points as the shared secret for generating the hashed MIC in the neighbor messages. To create an RF group, you configure all of the Cisco WLCs to be included in the group with the same RF group name.

If there is any possibility that an access point joined to a Cisco WLC may hear RF transmissions from an access point on a different Cisco WLC, you should configure the Cisco WLCs with the same RF group name. If RF transmissions between access points can be heard, then system-wide RRM is recommended to avoid 802.11 interference and contention as much as possible.

Mobility Controller

An MC can either be a group leader or a group member. One of the MCs can act as a RF group leader based on RF grouping and RF group election with other MCs. The order of priority to elect the RF leader is based on the maximum number of APs the controller or switch can support. The highest priority being 1 and the least being 5.

1. WiSM 2 Controllers
2. Cisco WLC 5700 Series Controllers
3. WiSM 1 Controllers
4. Catalyst 3850 Series Switches
5. Catalyst 3650 Series Switches

When one of the MCs becomes the RRM group leader, the remaining MCs become RRM group members. RRM group members send their RF information to the Group Leader. The group leader determines a channel and Tx power plan for the network and passes the information back to the RF group members. The MCs push the power plan to MA for the radios that belong to MA. These channel and power plans are ultimately pushed down to individual radios.

Note MC has MA functionality within it.

Mobility Agent

The MA communicates with the MC. The MC includes MAC or IP address of the switch/controller while communicating with the MA.

The MA provides the following information when polled by the MC:

- Interference or noise data.
- Neighbor data.
- Radio capabilities (supported channels, power levels).
- Radio configuration (power, channel, channel width).
- Radar data.

The MC exchanges the following information with the switch/controller (MA). The message includes:

- Configurations (channel/power/channel width) for individual radios.
- Polling requests for current configurations and RF measurements for individual radios
- Group Leader Update

In turn, the MA communicates the following messages with the MC:

- RF measurements from radios (e.g. load, noise and neighbor information)
- RF capabilities and configurations of individual radios

The MA sets channel, power, and channel width on the radios when directed by the MC. The DFS, coverage hole detection/mitigation, static channel/power configurations are performed by the MA.

Rogue Access Point Detection in RF Groups

After you have created an RF group of Cisco WLCs, you need to configure the access points connected to the Cisco WLCs to detect rogue access points. The access points will then select the beacon/probe-response frames in neighboring access point messages to see if they contain an authentication information element (IE) that matches that of the RF group. If the select is successful, the frames are authenticated. Otherwise, the authorized access point reports the neighboring access point as a rogue, records its BSSID in a rogue table, and sends the table to the Cisco WLC.

The AP has a RRM CAPWAP subsystem that exchanges messages with the mobility agent.

RRM components on the AP perform the following functions:

- AP measurements, such as interference (Wi-Fi), noise, coverage, and load, and client measurements.
- Radio neighbor discovery.
- Radar detection.
- Set various RF parameters (channel, channel width, transmit power control, and so on)

Transmit Power Control

The switch dynamically controls access point transmit power based on the real-time wireless LAN conditions.

The Transmit Power Control (TPC) algorithm both increases and decreases an access point's power in response to changes in the RF environment. In most instances, TPC seeks to lower an access point's power to reduce interference, but in the case of a sudden change in the RF coverage—for example, if an access point fails or becomes disabled—TPC can also increase power on surrounding access points. This feature is different from coverage hole detection, which is primarily concerned with clients. TPC provides enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

Overriding the TPC Algorithm with Minimum and Maximum Transmit Power Settings

The TPC algorithm balances RF power in many diverse RF environments. However, it is possible that automatic power control will not be able to resolve some scenarios in which an adequate RF design was not possible to implement due to architectural restrictions or site restrictions—for example, when all access points must be mounted in a central hallway, placing the access points close together, but requiring coverage out to the edge of the building.

In these scenarios, you can configure maximum and minimum transmit power limits to override TPC recommendations. The maximum and minimum TPC power settings apply to all access points through RF profiles in a RF network.

To set the Maximum Power Level Assignment and Minimum Power Level Assignment, enter the maximum and minimum transmit power used by RRM in the text boxes in the Tx Power Control page. The range for these parameters is -10 to 30 dBm. The minimum value cannot be greater than the maximum value; the maximum value cannot be less than the minimum value.

If you configure a maximum transmit power, RRM does not allow any access point attached to the switch to exceed this transmit power level (whether the power is set by RRM TPC or by coverage hole detection). For example, if you configure a maximum transmit power of 11 dBm, then no access point would transmit above 11 dBm, unless the access point is configured manually.

Dynamic Channel Assignment

Two adjacent access points on the same channel can cause either signal contention or signal collision. In a collision, data is not received by the access point. This functionality can become a problem, for example, when someone reading an e-mail in a café affects the performance of the access point in a neighboring business. Even though these are separate networks, someone sending traffic to the café on channel 1 can disrupt communication in an enterprise using the same channel. Switches can dynamically allocate access point channel assignments to avoid conflict, and increase capacity and performance. Channels are "reused" to avoid

wasting scarce RF resources. In other words, channel 1 is allocated to a different access point far from the café, which is more effective than not using channel 1 altogether.

The switch's Dynamic Channel Assignment (DCA) capabilities are also useful in minimizing adjacent channel interference between access points. For example, two overlapping channels in the 802.11b/g band, such as 1 and 2, cannot both simultaneously use 11/54 Mbps. By effectively reassigning channels, the switch keeps adjacent channels that are separated.

Note We recommend that you use only non-overlapping channels (1, 6, 11, and so on).

Note Channel change does not require you to shut down the radio.

The switch examines a variety of real-time RF characteristics to efficiently handle channel assignments as follows:

- Access point received energy—The received signal strength measured between each access point and its nearby neighboring access points. Channels are optimized for the highest network capacity.
- Noise—Noise can limit signal quality at the client and access point. An increase in noise reduces the effective cell size and degrades user experience. By optimizing channels to avoid noise sources, the switch can optimize coverage while maintaining system capacity. If a channel is unusable due to excessive noise, that channel can be avoided.
- 802.11 Interference—Interference is any 802.11 traffic that is not part of your wireless LAN, including rogue access points and neighboring wireless networks. Lightweight access points constantly scan all channels looking for sources of interference. If the amount of 802.11 interference exceeds a predefined configurable threshold (the default is 10 percent), the access point sends an alert to the switch. Using the RRM algorithms, the switch may then dynamically rearrange channel assignments to increase system performance in the presence of the interference. Such an adjustment could result in adjacent lightweight access points being on the same channel, but this setup is preferable to having the access points remain on a channel that is unusable due to an interfering foreign access point.

  In addition, if other wireless networks are present, the switch shifts the usage of channels to complement the other networks. For example, if one network is on channel 6, an adjacent wireless LAN is assigned to channel 1 or 11. This arrangement increases the capacity of the network by limiting the sharing of frequencies. If a channel has virtually no capacity remaining, the switch may choose to avoid this channel. In huge deployments in which all non-overlapping channels are occupied, the switch does its best, but you must consider RF density when setting expectations.
- Load and utilization—When utilization monitoring is enabled, capacity calculations can consider that some access points are deployed in ways that carry more traffic than other access points (for example, a lobby versus an engineering area). The switch can then assign channels to improve the access point with the worst performance reported. The load is taken into account when changing the channel structure to minimize the impact on clients currently in the wireless LAN. This metric keeps track of every access point's transmitted and received packet counts to determine how busy the access points are. New clients avoid an overloaded access point and associate to a new access point. This parameter is disabled by default.

The switch combines this RF characteristic information with RRM algorithms to make system-wide decisions. Conflicting demands are resolved using soft-decision metrics that guarantee the best choice for minimizing

network interference. The end result is optimal channel configuration in a three-dimensional space, where access points on the floor above and below play a major factor in an overall wireless LAN configuration.

Note Radios using 40MHz channels in the 2.4-GHz band or 80MHz channels are not supported by DCA.

The RRM startup mode is invoked in the following conditions:

- In a single-switch environment, the RRM startup mode is invoked after the switch is upgraded and rebooted.
- In a multiple-switch environment, the RRM startup mode is invoked after an RF Group leader is elected.

You can trigger the RRM startup mode from the CLI.

The RRM startup mode runs for 100 minutes (10 iterations at 10-minute intervals). The duration of the RRM startup mode is independent of the DCA interval, sensitivity, and network size. The startup mode consists of 10 DCA runs with high sensitivity (making channel changes easy and sensitive to the environment) to converge to a steady state channel plan. After the startup mode is finished, DCA continues to run at the specified interval and sensitivity.

Note DCA algorithm interval is set to one hour, but DCA algorithm always runs in default interval of 10min, channel allocation happens for every 10min interval for the first 10 cycles, and channel changes as per DCA algorithm for every 10min. After that it goes back to the configured time interval. This is common for both DCA interval and Anchor time since it follows the steady state.

Note If DCA/TPC is turned off on the RF-group member, and auto is set on RF-group leader, the channel/TX power on member gets changed as per the algorithm run on the RF-group leader.

Coverage Hole Detection and Correction

The RRM coverage hole detection algorithm can detect areas of radio coverage in a wireless LAN that are below the level needed for robust radio performance. This feature can alert you to the need for an additional (or relocated) lightweight access point.

If clients on a lightweight access point are detected at threshold levels (RSSI, failed client count, percentage of failed packets, and number of failed packets) lower than those specified in the RRM configuration, the access point sends a “coverage hole” alert to the switch. The alert indicates the existence of an area where clients are continually experiencing poor signal coverage, without having a viable access point to which to roam. The switch discriminates between coverage holes that can and cannot be corrected. For coverage holes that can be corrected, the switch mitigates the coverage hole by increasing the transmit power level for that specific access point. The switch does not mitigate coverage holes caused by clients that are unable to increase their transmit power or are statically set to a power level because increasing their downstream transmit power might increase interference in the network.

How to Configure RRM

Configuring Advanced RRM CCX Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm ccx location-measurement** *interval* **Example:** `Switch(config)# ap dot11 24ghz rrm ccx location-measurement 15`	Configures the interval for 802.11 CCX client location measurements. The range is from 10 to 32400 seconds.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Neighbor Discovery Type (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 2	**ap dot11 24ghz | 5ghz rrm ndp-type** {**protected | transparent**}
	Example:
	`Switch(config)#ap dot11 24ghz rrm ndp-type protected`
	`Switch(config)#ap dot11 24ghz rrm ndp-type transparent`
		Configures the neighbor discovery type. By default, the mode is set to "transparent".
		• **protected**—Sets the neighbor discover type to protected. Packets are encrypted.
		• **transparent**—Sets the neighbor discover type to transparent. Packets are sent as is.

	Command or Action	Purpose
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring RRM Profile Thresholds, Monitoring Channels, and Monitoring Intervals (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **802.11a/n/ac** > **RRM** > **General** or **Configuration** > **Wireless** > **802.11b/g/n** > **RRM** > **General** to open RRM General page.

Step 2 Configure profile thresholds used for alarming as follows:

Note The profile thresholds have no bearing on the functionality of the RRM algorithms. Switches send an SNMP trap (or an alert) to the Cisco Prime Infrastructure or another trap receiver when individual APs values set for these threshold parameters are exceeded.

a) In the **Interference** text box, enter the percentage of interference (802.11 traffic from sources outside of your wireless network) on a single access point. The valid range is 0 to 100%, and the default value is 10%.
b) In the **Clients** text box, enter the number of clients on a single access point. The valid range is 1 to 75, and the default value is 12.
c) In the **Noise** text box, enter the level of noise (non-802.11 traffic) on a single access point. The valid range is –127 to 0 dBm, and the default value is –70 dBm.
d) In the **Utilization** text box, enter the percentage of RF bandwidth being used by a single access point. The valid range is 0 to 100%, and the default value is 80%.
e) In the **Throughput** text box, enter the level of Throughput being used by a single access point. The valid range is 1000 to 10000000, and the default value is 1000000.

Step 3 From the **Channel List** drop-down list, choose one of the following options to specify the set of channels that the access point uses for RRM scanning:

- **All Channels**—RRM channel scanning occurs on all channels supported by the selected radio, which includes channels not allowed in the country of operation.
- **Country Channels**—RRM channel scanning occurs only on the data channels in the country of operation. This is the default value.
- **DCA Channels**—RRM channel scanning occurs only on the channel set used by the DCA algorithm, which by default includes all of the non-overlapping channels allowed in the country of operation. However, you can specify the channel set to be used by DCA if desired. To do so, follow instructions in the Dynamic Channel Assignment.

Step 4 Configure monitor intervals as follows:

1. In the **Channel Scan Interval** text box, enter (in seconds) the sum of the time between scans for each channel within a radio band. The entire scanning process takes 50 ms per channel, per radio and runs at

the interval configured here. The time spent listening on each channel is determined by the non-configurable 50-ms scan time and the number of channels to be scanned. For example, in the U.S. all 11 802.11b/g channels are scanned for 50 ms each within the default 180-second interval. So every 16 seconds, 50 ms is spent listening on each scanned channel (180/11 = ~16 seconds). The Channel Scan Interval parameter determines the interval at which the scanning occurs. The valid range is 60 to 3600 seconds, and the default value for 802.11a/n/ac and 802.11b/g/n radios is 180 seconds.

2. In the **Neighbor Packet Frequency** text box, enter (in seconds) how frequently neighbor packets (messages) are sent, which eventually builds the neighbor list. The valid range is 60 to 3600 seconds, and the default value is 60 seconds.

   Note If the access point radio does not receive a neighbor packet from an existing neighbor within 60 minutes, the Cisco WLC deletes that neighbor from the neighbor list.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Note Click **Set to Factory Default** if you want to return all of the Cisco WLC's RRM parameters to their factory-default values.

Configuring RF Groups

This section describes how to configure RF groups through either the GUI or the CLI.

Note The RF group name is generally set at deployment time through the Startup Wizard. However, you can change it as necessary.

Note When the multiple-country feature is being used, all Cisco WLCs intended to join the same RF group must be configured with the same set of countries, configured in the same order.

Note You can also configure RF groups using the Cisco Prime Infrastructure.

Configuring the RF Group Mode (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **802.11a/n/ac** > **RRM** > **RF Grouping** or or **Configuration** > **Wireless** > **802.11b/g/n** > **RRM** > **RF Grouping** to open the RF Grouping page.

Step 2 From the **Group Mode** drop-down list, choose the mode that you want to configure for this Cisco WLC.

You can configure RF grouping in the following modes:

- auto—Sets the RF group selection to automatic update mode.

  Note A configured static leader cannot become a member of another RF group until its mode is set to "auto".

- leader—Sets the RF group selection to static mode, and sets this Cisco WLC as the group leader.
- off—Sets the RF group selection off. Every Cisco WLC optimizes its own access point parameters.

  Note A Cisco WLC with a lower priority cannot assume the role of a group leader if a Cisco WLC with a higher priority is available. Here, priority is related to the processing power of the Cisco WLC.

  Note We recommend that Cisco WLCs participate in automatic RF grouping. You can override RRM settings without disabling automatic RF group participation.

Step 3 Click **Apply** to save the configuration and click **Restart** to restart the RRM RF Grouping algorithm.

Step 4 If you configured RF Grouping mode for this Cisco WLC as a static leader, you can add group members from the Group Members section as follows:

1. In the switch Name text box, enter the Cisco WLC that you want to add as a member to this group.
2. In the IP Address text box, enter the IP address of the Cisco WLC.
3. Click **Add** to add the member to this group.

   Note If the member has not joined the static leader, the reason of the failure is shown in parentheses.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Configuring RF Group Selection Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm group-mode** {**auto | leader | off**} **Example:** `Switch(config)#ap dot11 24ghz rrm group-mode leader`	Configures RF group selection mode for 802.11 bands. • **auto**—Sets the 802.11 RF group selection to automatic update mode. • **leader**—Sets the 802.11 RF group selection to leader mode.

	Command or Action	Purpose
		• **off**—Disables the 802.11 RF group selection.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring an RF Group Name (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wireless rf-network** *name* **Example:** `Switch (config)# wireless rf-network test1`	Creates an RF group. The group name should be ASCII String up to 19 characters and is case sensitive. **Note** Repeat this procedure for each controller that you want to include in the RF group.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 4	**show network profile** *profile_number*	Displays the RF group. **Note** You can view the network profile number from 1 to 4294967295.

Configuring an RF Group Name (GUI)

Procedure

Step 1 Choose **Configuration** > **Controller** > **General** to open the General page.

Step 2 Enter a name for the RF group in the RF Group Name text box. The name can contain up to 19 ASCII characters and is case sensitive.

Step 3 Click **Apply** to commit your changes.

Step 4 Click **Save Configuration** to save your changes.

Step 5 Repeat this procedure for each controller that you want to include in the RF group.

Configuring Members in a 802.11 Static RF Group (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm group-member** *group_name ip_addr* **Example:** `Switch(config)#ap dot11 24ghz rrm group-member Grpmem01 10.1.1.1`	Configures members in a 802.11 static RF group. The group mode should be set as leader for the group member to be active.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Transmit Power Control

Configuring the Tx-Power Control Threshold (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm tpc-threshold** *threshold_value* **Example:** `Switch(config)#ap dot11 24ghz rrm tpc-threshold -60`	Configures the Tx-power control threshold used by RRM for auto power assignment. The range is from –80 to –50.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring the Tx-Power Level (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm txpower** {*trans_power_level* | **auto** | **max** | **min** | **once**} **Example:** `Switch(config)#ap dot11 24ghz rrm txpower auto`	Configures the 802.11 tx-power level • **trans_power_level**—Sets the transmit power level. • **auto**—Enables auto-RF. • **max**—Configures the maximum auto-RF tx-power. • **min**—Configures the minimum auto-RF tx-power. • **once**—Enables one-time auto-RF.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Transmit Power Control (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **802.11a/n/ac** > **RRM** > **TPC** or **Configuration** > **Wireless** > **802.11b** > **RRM** > **TPC** to open RRM Tx Power Control (TPC) page.

Step 2 Choose the Transmit Power Control.

Coverage Optimal Mode (TPCv1)— Offers strong signal coverage and stability. In this mode, power can be kept low to gain extra capacity and reduce interference.

Step 3 Choose one of the following options from the Power Level Assignment Method list to specify the Cisco WLC's dynamic power assignment mode:

- **Automatic**—Causes the Cisco WLC to periodically evaluate and, if necessary, update the transmit power for all joined access points. This is the default value.
- **On Demand**—Causes the Cisco WLC to periodically evaluate the transmit power for all joined access points. However, the Cisco WLC updates the power, if necessary, only when you click **Apply** after choosing **On Demand**.

Note The Cisco WLC does not evaluate and update the transmit power immediately when you click **Apply** after choosing **On Demand**. It waits for the next 600-second interval. This value is not configurable.

- **Fixed**—Prevents the Cisco WLC from evaluating and, if necessary, updating the transmit power for joined access points. The power level is set to the fixed value chosen from the drop-down list. The corresponding option for **Fixed** when you try to configure from CLI is **once**.

  Note The transmit power level is assigned an integer value instead of a value in mW or dBm. The integer corresponds to a power level that varies depending on the regulatory domain, channel, and antennas in which the access points are deployed.

  Note For optimal performance, we recommend that you use the Automatic setting.

Step 4 Enter the maximum and minimum power level assignment values in the Maximum Power Level Assignment and Minimum Power Level Assignment text boxes.

The range for the Maximum Power Level Assignment is –10 to 30 dBm.

The range for the Minimum Power Level Assignment is –10 to 30 dBm.

Step 5 In the Power Threshold text box, enter the cutoff signal level used by RRM when determining whether to reduce an access point's power. The default value for this parameter is –70 dBm for TPCv1, but can be changed when access points are transmitting at higher (or lower) than desired power levels.

The range for this parameter is –80 to –50 dBm. Increasing this value (between –65 and –50 dBm) causes the access points to operate at a higher transmit power. Decreasing the value has the opposite effect.

In applications with a dense population of access points, it may be useful to decrease the threshold to –80 or –75 dBm to reduce the number of BSSIDs (access points) and beacons seen by the wireless clients. Some wireless clients might have difficulty processing a large number of BSSIDs or a high beacon rate and might exhibit problematic behavior with the default threshold.

This page also shows the following nonconfigurable transmit power level parameter settings:

- Power Neighbor Count—The minimum number of neighbors an access point must have for the transmit power control algorithm to run.
- Power Assignment Leader—The MAC address of the RF group leader, which is responsible for power level assignment.
- Last Power Level Assignment—The last time RRM evaluated the current transmit power level assignments.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Configuring 802.11 RRM Parameters

Configuring Advanced 802.11 Channel Assignment Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event sensitivity** {**high** | **low** | **medium**} **Example:** `Switch(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high`	Configures CleanAir event-driven RRM parameters. • **High**–Specifies the most sensitivity to non-Wi-Fi interference as indicated by the air quality (AQ) value. • **Low**–Specifies the least sensitivity to non-Wi-Fi interference as indicated by the AQ value. • **Medium**–Specifies medium sensitivity to non-Wi-Fi interference as indicated by the AQ value.

Step 3	**ap dot11** {**24ghz** | **5ghz**} **rrm channel dca** {*channel number* | **anchor-time** | **global** {**auto** | **once**} | **interval** | **min-metric** | **sensitivity** {**high** | **low** | **medium**}}
	Example:
	`Switch(config)#ap dot11 24ghz rrm channel dca interval 2`
		Configures Dynamic Channel Assignment (DCA) algorithm parameters for the 802.11 band.
		• ***<1-14>***–Enter a channel number to be added to the DCA list.
		• **anchor-time**–Configures the anchor time for the DCA. The range is between 0 and 23 hours.
		• **global**–Configures the DCA mode for all 802.11 Cisco APs.
		  • **auto**–Enables auto-RF.
		  • **once**–Enables auto-RF only once.
		• **interval**–Configures the DCA interval value. The values are 1, 2, 3, 4, 6, 8, 12 and 24 hours and the default value 0 denotes 10 minutes.
		• **min-metric**–Configures the DCA minimum RSSI energy metric. The range is between -100 and -60.

	Command or Action	Purpose
		• **sensitivity**–Configures the DCA sensitivity level to changes in the environment. • **high**–Specifies the most sensitivity. • **low**–Specifies the least sensitivity. • **medium**–Specifies medium sensitivity.
Step 4	**ap dot11 5ghz rrm channel dca chan-width** {**20** | **40** | **80**} **Example:** `Switch(config)#ap dot11 5ghz rrm channel dca chan-width best maximum 20`	Configures the DCA channel bandwidth for all 802.11 radios in the 5-GHz band. Sets the channel bandwidth to 20 MHz, 40 MHz, or 80 MHz, ; 20 MHz is the default value for channel bandwidth. 80 MHz is the default value for best. Set the channel bandwidth to best before configuring the constraints.
Step 5	**ap dot11** {**24ghz** | **5ghz**} **rrm channel dca** {{**add** | **remove**} *channel_number* | **anchor-time** | **global** {**auto** | **once**} | **interval** | **min-metric** | **sensitivity** {**high** | **low** | **medium**}} **Example:** `Switch(config)#ap dot11 24ghz rrm channel dca interval 2`	Configures dynamic channel assignment (DCA) algorithm parameters for the 802.11 band. • **add** *channel_number*–Enter a channel number to be added to the DCA list. The *channel_number* ranges from 1 to 14. • **anchor-time**–Configures the anchor time for the DCA. The range is between 0 and 23 hours. • **global**–Configures the DCA mode for all 802.11 Cisco APs. • **auto**–Runs auto-RF. • **once**–Runs auto-RF only once. • **interval**– Configures the DCA interval value. The values are 1, 2, 3, 4, 6, 8, 12 and 24 hours and the default value 0 denotes 10 minutes. • **min-metric**–Configures the DCA minimum RSSI energy metric. The range is between -100 and -60. • **sensitivity**–Configures the DCA sensitivity level to changes in the environment. • **high**–Specifies the most sensitivity. • **low**–Specifies the least sensitivity.

	Command or Action	Purpose
		• **medium**–Specifies medium sensitivity.
Step 6	**ap dot11 {24ghz | 5ghz} rrm channel device** **Example:** `Switch(config)#ap dot11 24ghz rrm channel device`	Configures the persistent non-Wi-Fi device avoidance in the 802.11 channel assignment.
Step 7	**ap dot11 {24ghz | 5ghz} rrm channel foreign** **Example:** `Switch(config)#ap dot11 24ghz rrm channel foreign`	Configures the foreign AP 802.11 interference avoidance in the channel assignment.
Step 8	**ap dot11 {24ghz | 5ghz} rrm channel load** **Example:** `Switch(config)#ap dot11 24ghz rrm channel load`	Configures the Cisco AP 802.11 load avoidance in the channel assignment.
Step 9	**ap dot11 {24ghz | 5ghz} rrm channel noise** **Example:** `Switch(config)#ap dot11 24ghz rrm channel noise`	Configures the 802.11 noise avoidance in the channel assignment.
Step 10	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Dynamic Channel Assignment (GUI)

You can specify the channels that the Dynamic Channel Assignment (DCA) algorithm considers when selecting the channels to be used for RRM scanning by using the Cisco WLC GUI.

Note This functionality is helpful when you know that the clients do not support certain channels because they are legacy devices or they have certain regulatory restrictions.

Procedure

Step 1 Disable the 802.11a/n/ac or 802.11b/g/n network as follows:

a) Choose **Configuration** > **Wireless** > **802.11a/n/ac** > **Network** or **Configuration** > **Wireless** > **802.11b/g/n** > **Network** to open the Global Parameters page.

b) Unselect the **802.11a/n/ac** (or **802.11b/g/n**) **Network Status** check box.
c) Click **Apply**.

Step 2 Choose **Configuration** > **Wireless** > **802.11a/n/ac** > **RRM** > **DCA** or **Configuration** > **Wireless** > **802.11b/g/n** > **RRM** > **DCA** to open the Dynamic Channel Assignment (DCA) page.

Step 3 Choose one of the following options from the **Channel Assignment Method** drop-down list to specify the Cisco WLC's DCA mode:

- **Automatic**—Causes the Cisco WLC to periodically evaluate and, if necessary, update the channel assignment for all joined access points. This is the default value.
- **Freeze**—Causes the Cisco WLC to evaluate and update the channel assignment for all joined access points, if necessary, only when you click **Apply** after selecting the **Freeze** option.

  Note The Cisco WLC does not evaluate and update the channel assignment immediately when you click **Apply** after selecting the **Freeze** option. It waits for the next interval to elapse.

- **OFF**—Turns off DCA and sets all access point radios to the first channel of the band. If you choose this option, you must manually assign channels on all radios.

  Note For optimal performance, we recommend that you use the Automatic setting.

Step 4 From the Interval drop-down list, choose one of the following options to specify how often the DCA algorithm is allowed to run: **10 minutes**, **1 hour**, **2 hours**, **3 hours**, **4 hours**, **6 hours**, **8 hours**, **12 hours**, or **24 hours**. The default value is 10 minutes.

Step 5 From the AnchorTime drop-down list, choose a number to specify the time of day when the DCA algorithm is to start. The options are numbers between 0 and 23 (inclusive) representing the hour of the day from 12:00 a.m. to 11:00 p.m.

Step 6 Check the **Avoid Foreign AP Interference** check box to cause the Cisco WLC's RRM algorithms to consider 802.11 traffic from foreign access points (those not included in your wireless network) when assigning channels to lightweight access points, or unselect it to disable this feature. For example, RRM may adjust the channel assignment to have access points avoid channels close to foreign access points. The default value is selected.

Step 7 Select the **Avoid Cisco AP Load** check box to cause the Cisco WLC's RRM algorithms to consider 802.11 traffic from Cisco lightweight access points in your wireless network when assigning channels, or unselect it to disable this feature. For example, RRM can assign better reuse patterns to access points that carry a heavier traffic load. The default value is unselected.

Step 8 Select the **Avoid Non-802.11a (802.11b) Noise** check box to cause the Cisco WLC's RRM algorithms to consider noise (non-802.11 traffic) in the channel when assigning channels to lightweight access points, or unselect it to disable this feature. For example, RRM may have access points avoid channels with significant interference from nonaccess point sources, such as microwave ovens. The default value is selected.

Step 9 Select the **Avoid Persistent Non-WiFi Interference** check box to enable the Cisco WLC to ignore persistent non-Wi-Fi interference.

Step 10 From the **DCA Channel Sensitivity** drop-down list, choose one of the following options to specify how sensitive the DCA algorithm is to environmental changes such as signal, load, noise, and interference when determining whether to change channels:

- **Low**—The DCA algorithm is not particularly sensitive to environmental changes.
- **Medium**—The DCA algorithm is moderately sensitive to environmental changes.
- **High**—The DCA algorithm is highly sensitive to environmental changes.

The default value is Medium. The DCA sensitivity thresholds vary by radio band, as noted in the following table:

Table 47: DCA Sensitivity Thresholds

Option	2.4-GHz DCA Sensitivity Threshold	5-GHz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	10 dB	15 dB
Low	20 dB	20 dB

Step 11 For 802.11a/n/ac networks only, choose one of the following channel width options to specify the channel bandwidth supported for all 802.11n radios in the 5-GHz band:

- **20 MHz**—The 20-MHz channel bandwidth (default)
- **40 MHz**—The 40-MHz channel bandwidth

  Note If you choose 40 MHz, be sure to choose at least two adjacent channels from the DCA Channel List in *Step 13* (for example, a primary channel of 36 and an extension channel of 40). If you choose only one channel, that channel is not used for 40-MHz channel width.

  Note If you choose 40 MHz, you can also configure the primary and extension channels used by individual access points.

  Note To override the globally configured DCA channel width setting, you can statically configure an access point's radio for 20- or 40-MHz mode in the 802.11a/n Cisco APs > Configure page. if you then change the static RF channel assignment method to WLC Controlled on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.

  Note If you choose 40 MHz on the A radio, you cannot pair channels 116, 140, and 165 with any other channels.

- **80 MHz**—The 80-MHz bandwidth for the 802.11ac radios.

  Note If you choose 80 MHz, be sure to choose four adjacent channels from the DCA Channel List in *Step 13* (for example, a primary channel of 36 and an extension channel of 40). If you choose only one channel, that channel is not used for 40-MHz channel width.

  Note If you choose 80 MHz, you can also configure the primary and extension channels used by individual access points.

  Note To override the globally configured DCA channel width setting, you can statically configure an access point's radio for 20-, 40-, or 80-MHz mode on the 802.11a/n Cisco APs > Configure page. if you then change the static RF channel assignment method to WLC Controlled on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.

Note If you choose 40 MHz on the A radio, you cannot pair channels 116, 140, and 165 with any other channels.

This page also shows the following nonconfigurable channel parameter settings:

- Channel Assignment Leader—The MAC address of the RF group leader, which is responsible for channel assignment.
- Last Auto Channel Assignment—The last time RRM evaluated the current channel assignments. This is used only for RF leader and not for the RF member.

Step 12 In the DCA Channel List area, the DCA Channels text box shows the channels that are currently selected. To choose a channel, select its check box in the Select column. To exclude a channel, unselect its check box.

The ranges are as follows:

- 802.11a—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 165 (depending on countries).
- 802.11b/g—1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 (depending on countries).

The defaults are as follows:

- 802.11a—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161
- 802.11b/g—1, 6, 11

Step 13 Click **Apply**.

Step 14 Reenable the 802.11 networks as follows:

1. Choose **Configuration** > **Wireless** > **802.11a/n/ac** > **Network** or **Configuration** > **Wireless** > **802.11b/g/n** > **Network** to open the Global Parameters page.
2. Select the **802.11a/n/ac** (or **802.11b/g/n**) **Network Status** check box.
3. Click **Apply**.

Step 15 Click **Save Configuration**.

Configuring 802.11 Coverage Hole Detection (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ap dot11 24ghz | 5ghz rrm coverage data{fail-percentage | packet-count | rssi-threshold}** **Example:** `Switch(config)#ap dot11 24ghz rrm coverage data fail-percentage 60`	Configures the 802.11 coverage hole detection for data packets. • **fail-percentage**—Configures the 802.11 coverage failure-rate threshold for uplink data packets as a percentage that ranges from 1 to 100%. • **packet-count**—Configures the 802.11 coverage minimum failure count threshold for uplink data packets that ranges from 1 to 255. • **rssi-threshold**—Configures the 802.11 minimum receive coverage level for data packets that range from –90 to –60 dBm.
Step 3	**ap dot11 24ghz | 5ghz rrm coverage exception global** *exception level* **Example:** `Switch(config)#ap dot11 24ghz rrm coverage exception global 50`	Configures the 802.11 Cisco AP coverage exception level as a percentage that ranges from 0 to 100%.
Step 4	**ap dot11 24ghz | 5ghz rrm coverage level global** *cli_min exception level* **Example:** `Switch(config)#ap dot11 24ghz rrm coverage level global 10`	Configures the 802.11 Cisco AP client minimum exception level that ranges from 1 to 75 clients.
Step 5	**ap dot11 24ghz | 5ghz rrm coverage voice{fail-percentage | packet-count | rssi-threshold}** **Example:** `Switch(config)#ap dot11 24ghz rrm coverage voice packet-count 10`	Configures the 802.11 coverage hole detection for voice packets. • **fail-percentage**—Configures the 802.11 coverage failure-rate threshold for uplink voice packets as a percentage that ranges from 1 to 100%. • **packet-count**—Configures the 802.11 coverage minimum failure count threshold for uplink voice packets that ranges from 1 to 255. • **rssi-threshold**—Configures the 802.11 minimum receive coverage level for voice packets that range from –90 to –60 dBm.

	Command or Action	Purpose
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Coverage Hole Detection (GUI)

Procedure

Step 1 Disable the 802.11 network as follows:

a) Choose **Configuration** > **Wireless** > **802.11a/n/ac** or **Configuration** > **Wireless** > **802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Global Parameters page.

b) Unselect the **802.11a/n/ac** (or **802.11b/g/n**) **Network Status** check box.

c) Click **Apply**.

Step 2 Choose **Configuration** > **Wireless** > **802.11a/n/ac** > **RRM** > **Coverage Thresholds** or **Configuration** > **Wireless** > **802.11b/g/n** > **RRM** > **Coverage Thresholds** to open coverage page.

Step 3 Select the **Enable Coverage Hole Detection** check box to enable coverage hole detection, or unselect it to disable this feature. If you enable coverage hole detection, the Cisco WLC automatically determines, based on data received from the access points, if any access points have clients that are potentially located in areas with poor coverage. The default value is selected.

Step 4 In the **Data RSSI** text box, enter the minimum Receive Signal Strength Indication (RSSI) value for data packets received by the access point. The value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. If the access point receives a packet in the data queue with an RSSI value below the value that you enter here, a potential coverage hole has been detected. The valid range is –90 to –60 dBm, and the default value is –80 dBm. The access point takes data RSSI measurements every 5 seconds and reports them to the Cisco WLC in 90-second intervals.

Step 5 In the **Voice RSSI** text box, enter the minimum Receive Signal Strength Indication (RSSI) value for voice packets received by the access point. The value that you enter is used to identify coverage holes within your network. If the access point receives a packet in the voice queue with an RSSI value below the value that you enter here, a potential coverage hole has been detected. The valid range is –90 to –60 dBm, and the default value is –80 dBm. The access point takes voice RSSI measurements every 5 seconds and reports them to the Cisco WLC in 90-second intervals.

Step 6 In the **Min Failed Client Count per AP** text box, enter the minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold. The valid range is 1 to 75, and the default value is 3.

Step 7 In the **Coverage Exception Level per AP** text box, enter the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point. The valid range is 0 to 100%, and the default value is 25%.

Note If both the number and percentage of failed packets exceed the values configured for Failed Packet Count and Failed Packet Percentage (configurable through the Cisco WLC CLI) for a 5-second period, the client is considered to be in a pre-alarm condition. The Cisco WLC uses this information to distinguish between real and false coverage holes. False positives are generally due to the poor roaming logic implemented on most clients. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the Min Failed Client Count per AP and Coverage Exception Level per AP text boxes over two 90-second periods (a total of 180 seconds). The Cisco WLC determines if the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Step 8 Click **Apply**.

Step 9 Reenable the 802.11 network as follows:

a) Choose **Configuration** > **Wireless** > **802.11a/n/ac** > **Network** or **Configuration** > **Wireless** > **802.11b/g/n** > **Network** to open the 802.11a (or 802.11b/g) Global Parameters page.

b) Select the **802.11a/n/ac** (or **802.11b/g/n**) **Network Status** check box.

c) Click **Apply**.

Step 10 Click **Save Configuration**.

Configuring 802.11 Event Logging (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 2	**ap dot11 24ghz | 5ghz rrm logging**{**channel | coverage | foreign | load | noise | performance | txpower**}
	Example:
	`Switch(config)#ap dot11 24ghz rrm logging channel`
	`Switch(config)#ap dot11 24ghz rrm logging coverage`
	`Switch(config)#ap dot11 24ghz rrm logging foreign`
	`Switch(config)#ap dot11 24ghz rrm logging load`
	`Switch(config)#ap dot11 24ghz rrm logging noise`
	`Switch(config)#ap dot11 24ghz rrm logging performance`
		Configures event-logging for various parameters.
		• **channel**—Configures the 802.11 channel change logging mode.
		• **coverage**—Configures the 802.11 coverage profile logging mode.
		• **foreign**—Configures the 802.11 foreign interference profile logging mode.
		• **load**—Configures the 802.11 load profile logging mode.
		• **noise**—Configures the 802.11 noise profile logging mode.
		• **performance**—Configures the 802.11 performance profile logging mode.
		• **txpower**—Configures the 802.11 transmit power change logging mode.

	Command or Action	Purpose
	`Switch(config)#ap dot11 24ghz rrm logging txpower`	
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring 802.11 Statistics Monitoring (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm monitor channel-list**{**all | country | dca**} **Example:** `Switch(config)#ap dot11 24ghz rrm monitor channel-list all`	Sets the 802.11 monitoring channel-list for parameters such as noise/interference/rogue. • **all**— Monitors all channels. • **country**— Monitor channels used in configured country code. • **dca**— Monitor channels used by dynamic channel assignment.
Step 3	**ap dot11 24ghz | 5ghz rrm monitor coverage** *interval* **Example:** `Switch(config)#ap dot11 24ghz rrm monitor coverage 600`	Configures the 802.11 coverage measurement interval in seconds that ranges from 60 to 3600.
Step 4	**ap dot11 24ghz | 5ghz rrm monitor load** *interval* **Example:** `Switch(config)#ap dot11 24ghz rrm monitor load 180`	Configures the 802.11 load measurement interval in seconds that ranges from 60 to 3600.
Step 5	**ap dot11 24ghz | 5ghz rrm monitor noise** *interval* **Example:** `Switch(config)#ap dot11 24ghz rrm monitor noise 360`	Configures the 802.11 noise measurement interval (channel scan interval) in seconds that ranges from 60 to 3600.

	Command or Action	Purpose
Step 6	**ap dot11 24ghz | 5ghz rrm monitor signal** *interval* **Example:** `Switch(config)#ap dot11 24ghz rrm monitor signal 480`	Configures the 802.11 signal measurement interval (neighbor packet frequency) in seconds that ranges from 60 to 3600.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring the 802.11 Performance Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm profile clients** *cli_threshold_value* **Example:** `Switch(config)#ap dot11 24ghz rrm profile clients 20`	Sets the threshold value for 802.11 Cisco AP clients that range between 1 and 75 clients.
Step 3	**ap dot11 24ghz | 5ghz rrm profile foreign** *int_threshold_value* **Example:** `Switch(config)#ap dot11 24ghz rrm profile foreign 50`	Sets the threshold value for 802.11 foreign interference that ranges between 0 and 100%.
Step 4	**ap dot11 24ghz | 5ghz rrm profile noise** *for_noise_threshold_value* **Example:** `Switch(config)#ap dot11 24ghz rrm profile noise -65`	Sets the threshold value for 802.11 foreign noise ranges between –127 and 0 dBm.
Step 5	**ap dot11 24ghz | 5ghz rrm profile throughput** *throughput_threshold_value* **Example:**	Sets the threshold value for 802.11 Cisco AP throughput that ranges between 1000 and 10000000 bytes per second.

	Command or Action	Purpose
	`Switch(config)#ap dot11 24ghz rrm profile throughput 10000`	
Step 6	**ap dot11 24ghz | 5ghz rrm profile utilization** *rf_util_threshold_value* **Example:** `Switch(config)#ap dot11 24ghz rrm profile utilization 75`	Sets the threshold value for 802.11 RF utilization that ranges between 0 to 100%.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Rogue Access Point Detection in RF Groups

Configuring Rogue Access Point Detection in RF Groups (CLI)

Before you begin

Ensure that each Cisco WLC in the RF group has been configured with the same RF group name.

Note The name is used to verify the authentication IE in all beacon frames. If the Cisco WLCs have different names, false alarms will occur.

Procedure

	Command or Action	Purpose
Step 1	**ap name** *Cisco_AP* **mode** {**local** | **monitor**} **Example:** `Switch# ap name ap1 mode local`	Configures a particular access point for local (normal) mode or monitor (listen-only) mode. Perform this step for every access point connected to the Cisco WLC.
Step 2	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 3	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 4	**wireless wps ap-authentication** **Example:**	Enables rogue access point detection.

	Command or Action	Purpose
	`Switch (config)# wireless wps ap-authentication`	
Step 5	**wireless wps ap-authentication threshold** *value* **Example:** `Switch (config)# wireless wps ap-authentication threshold 50`	Specifies when a rogue access point alarm is generated. An alarm occurs when the threshold value (which specifies the number of access point frames with an invalid authentication IE) is met or exceeded within the detection period. The valid threshold range is from 1 to 255, and the default threshold value is 1. To avoid false alarms, you may want to set the threshold to a higher value. **Note** Enable rogue access point detection and threshold value on every Cisco WLC in the RF group. **Note** If rogue access point detection is not enabled on every Cisco WLC in the RF group, the access points on the Cisco WLCs with this feature disabled are reported as rogues.

Enabling Rogue Access Point Detection in RF Groups (GUI)

Procedure

Step 1 Make sure that each Cisco WLC in the RF group has been configured with the same RF group name.

Note The name is used to verify the authentication IE in all beacon frames. If the Cisco WLCs have different names, false alarms will occur.

Step 2 Choose **Configuration** > **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 3 Click the name of an access point to open the All APs > Edit page.

Step 4 Choose either **local** or **monitor** from the AP Mode drop-down list and click **Apply** to commit your changes.

Step 5 Click **Save Configuration** to save your changes.

Step 6 Repeat Step 2 through Step 5 for every access point connected to the Cisco WLC.

Step 7 Choose **Configuration** > **Security** > **Wireless Protection Policies** > **AP Authentication/MFP** to open the AP Authentication Policy page.

The name of the RF group to which this Cisco WLC belongs appears at the top of the page.

Step 8 Choose **AP Authentication** from the Protection Type drop-down list to enable rogue access point detection.

Step 9 Enter a number in the Alarm Trigger Threshold edit box to specify when a rogue access point alarm is generated. An alarm occurs when the threshold value (which specifies the number of access point frames with an invalid authentication IE) is met or exceeded within the detection period.

Note The valid threshold range is from1 to 255, and the default threshold value is 1. To avoid false alarms, you may want to set the threshold to a higher value.

Step 10 Click **Apply** to commit your changes.

Step 11 Click **Save Configuration** to save your changes.

Step 12 Repeat this procedure on every Cisco WLC in the RF group.

Note If rogue access point detection is not enabled on every Cisco WLC in the RF group, the access points on the Cisco WLCs with this feature disabled are reported as rogues.

Monitoring RRM Parameters and RF Group Status

Monitoring RRM Parameters

Table 48: Commands for monitoring Radio Resource Management

Commands	Description
show ap dot11 24ghz ccx	Displays the 802.11b CCX information for all Cisco APs.
show ap dot11 24ghz channel	Displays the configuration and statistics of the 802.11b channel assignment.
show ap dot11 24ghz coverage	Displays the configuration and statistics of the 802.11b coverage.
show ap dot11 24ghz group	Displays the configuration and statistics of the 802.11b grouping.
show ap dot11 24ghz l2roam	Displays 802.11b l2roam information.
show ap dot11 24ghz logging	Displays the configuration and statistics of the 802.11b event logging.
show ap dot11 24ghz monitor	Displays the configuration and statistics of the 802.11b monitoring.
show ap dot11 24ghz profile	Displays 802.11b profiling information for all Cisco APs.
show ap dot11 24ghz receiver	Displays the configuration and statistics of the 802.11b receiver.
show ap dot11 24ghz summary	Displays the configuration and statistics of the 802.11b Cisco APs.
show ap dot11 24ghz txpower	Displays the configuration and statistics of the 802.11b transmit power control.
show ap dot11 5ghz ccx	Displays 802.11a CCX information for all Cisco APs.
show ap dot11 5ghz channel	Displays the configuration and statistics of the 802.11a channel assignment.
show ap dot11 5ghz coverage	Displays the configuration and statistics of the 802.11a coverage.
show ap dot11 5ghz group	Displays the configuration and statistics of the 802.11a grouping.

Commands	Description
show ap dot11 5ghz l2roam	Displays 802.11a l2roam information.
show ap dot11 5ghz logging	Displays the configuration and statistics of the 802.11a event logging.
show ap dot11 5ghz monitor	Displays the configuration and statistics of the 802.11a monitoring.
show ap dot11 5ghz profile	Displays 802.11a profiling information for all Cisco APs.
show ap dot11 5ghz receiver	Displays the configuration and statistics of the 802.11a receiver.
show ap dot11 5ghz summary	Displays the configuration and statistics of the 802.11a Cisco APs.
show ap dot11 5ghz txpower	Displays the configuration and statistics of the 802.11a transmit power control.

Monitoring RF Group Status (CLI)

This section describes the new commands for RF group status.

The following commands can be used to monitor RF group status on the switch.

Table 49: Monitoring Aggressive Load Balancing Command

Command	Purpose
show ap dot11 5ghz group	Displays the Cisco WLC name which is the RF group leader for the 802.11a RF network.
show ap dot11 24ghz group	Displays the Cisco WLC name which is the RF group leader for the 802.11b/g RF network.

Monitoring RF Group Status (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **802.11a/n/ac** > **or 802.11b/g/n > RRM** > **RF Grouping** to open the RF Grouping Algorithm page.

This page shows the details of the RF group, displaying the configurable parameter **Group mode**, the **Group role** of this Cisco WLC, the **Group Update Interval** and the Cisco WLC name and IP address of the **Group Leader** to this Cisco WLC.

Note RF grouping mode can be set using the **Group Mode** drop-down list.

Tip Once a Cisco WLC has joined as a static member and you want to change the grouping mode, we recommend that you remove the member from the configured static-leader and also make sure that a member Cisco WLC has not been configured to be a member on multiple static leaders. This is to avoid repeated join attempts from one or more RF static leaders.

Step 2 (Optional) Repeat this procedure for the network type that you did not select (802.11a/n/ac or 802.11b/g/n).

Examples: RF Group Configuration

This example shows how to configure RF group name:

```
Switch# configure terminal
Switch(config)# wireless rf-network test1
Switch(config)# ap dot11 24ghz shutdown
Switch(config)# end
Switch # show network profile 5
```

This example shows how to configure rogue access point detection in RF groups:

```
Switch# ap name ap1 mode local
Switch# end
Switch# configure terminal
Switch(config)# wireless wps ap-authentication
Switch(config)# wireless wps ap-authentication threshold 50
Switch(config)# end
```

Information About ED-RRM

Spontaneous interference is interference that appears suddenly on a network, perhaps jamming a channel or a range of channels completely. The Cisco CleanAir spectrum event-driven RRM feature allows you to set a threshold for air quality (AQ) that, if exceeded, triggers an immediate channel change for the affected access point. Most RF management systems can avoid interference, but this information takes time to propagate through the system. Cisco CleanAir relies on AQ measurements to continuously evaluate the spectrum and can trigger a move within 30 seconds. For example, if an access point detects interference from a video camera, it can recover by changing channels within 30 seconds of the camera becoming active. Cisco CleanAir also identifies and locates the source of interference so that more permanent mitigation of the device can be performed at a later time.

Configuring ED-RRM on the Cisco Wireless LAN Controller (CLI)

Procedure

Step 1 Trigger spectrum event-driven radio resource management (RRM) to run when a Cisco CleanAir-enabled access point detects a significant level of interference by entering these commands:

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event** —Configures CleanAir driven RRM parameters for the 802.11 Cisco lightweight access points.

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event sensitivity** {**low** | **medium** | **high** | **custom**}—Configures CleanAir driven RRM sensitivity for the 802.11 Cisco lightweight access points. Default selection is Medium.

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event rogue-contribution**—Enables rogue contribution.

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event rogue-contribution duty-cycle** *thresholdvalue*—Configures threshold value for rogue contribution. The valid range is from 1 to 99, with 80 as the default.

Step 2 Save your changes by entering this command:

write memory

Step 3 See the CleanAir configuration for the 802.11a/n/ac or 802.11b/g/n network by entering this command:

show ap dot11 {**24ghz** | **5ghz**} **cleanair config**

Information similar to the following appears:

```
AdditionalClean Air Settings:
CleanAir Event-driven RRM State.............. : Enabled
CleanAir Driven RRM Sensitivity.............. : LOW
CleanAir Event-driven RRM Rogue Option....... : Enabled
CleanAir Event-driven RRM Rogue Duty Cycle... : 80
CleanAir Persistent Devices state............ : Disabled
CleanAir Persistent Device Propagation....... : Disabled
```

Configuring ED-RRM (GUI)

Procedure

Step 1 Choose **Configure** > **Radio Configurations** > **2.4 GHZ or 5 GHZ** > **RRM** > **DCA** to open the ED-RRM page.

Note Before enabling ED-RRM, you have to disable Network Status from **Configure** > **Radio Configurations** > **2.4 GHZ or 5 GHZ** > **Network** > **General** page, and then re-enable the network after configuring ED-RRM.

Step 2 In the Event Driven RRM section, select the **EDRRM** check box to reveal ED-RRM parameters .

Step 3 From the Sensitivity Threshold drop-down, select the value.

Options are: Low, Medium, or High. Default selection is Medium.

Note In the Show running configuration, the Sensitivity Threshold value selected by default is not visible.

Step 4 Select the **Rogue Contribution** check box to reveal Rogue Duty-Cycle parameters .

Step 5 Enter the **Rogue Duty Cycle** value in the text box.

The valid range is from 1 to 99, with 80 as the default.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Additional References for Radio Resource Management

Related Documents

Related Topic	Document Title
RRM commands and their details	*RRM Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)RRM Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

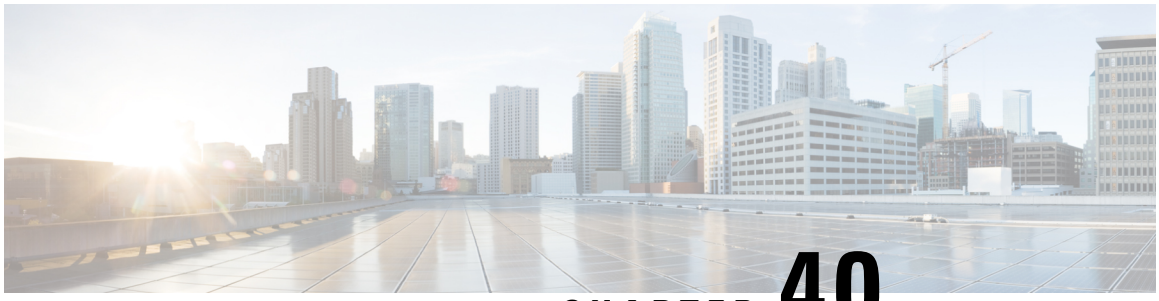
Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Performing Radio Resource Management Configuration

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.

PART XI

Security



CHAPTER 40

Preventing Unauthorized Access

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Preventing Unauthorized Access

You can prevent unauthorized users from reconfiguring your switch and viewing configuration information. Typically, you want network administrators to have access to your switch while you restrict access to users who dial from outside the network through an asynchronous port, connect from outside the network through a serial port, or connect through a terminal or workstation from within the local network.

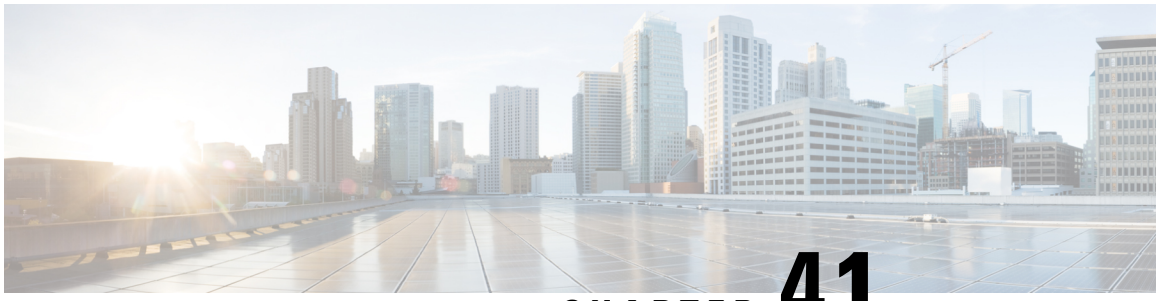
To prevent unauthorized access into your switch, you should configure one or more of these security features:

- At a minimum, you should configure passwords and privileges at each switch port. These passwords are locally stored on the switch. When users attempt to access the switch through a port or line, they must enter the password specified for the port or line before they can access the switch.
- For an additional layer of security, you can also configure username and password pairs, which are locally stored on the switch. These pairs are assigned to lines or ports and authenticate each user before that user can access the switch. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.
- If you want to use username and password pairs, but you want to store them centrally on a server instead of locally, you can store them in a database on a security server. Multiple networking devices can then use the same database to obtain user authentication (and, if necessary, authorization) information.

- You can also enable the login enhancements feature, which logs both failed and unsuccessful login attempts. Login enhancements can also be configured to block future login attempts after a set number of unsuccessful attempts are made. For more information, see the Cisco IOS Login Enhancements documentation.

Related Topics

Configuring Username and Password Pairs, on page 762
TACACS+ and Switch Access, on page 771
Setting a Telnet Password for a Terminal Line, on page 760



CHAPTER 41

Controlling Switch Access with Passwords and Privilege Levels

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Controlling Switch Access with Passwords and Privileges

The following are the restrictions for controlling switch access with passwords and privileges:

- Disabling password recovery will not work if you have set the switch to boot up manually by using the **boot manual** global configuration command. This command produces the boot loader prompt (*switch:*) after the switch is power cycled.

Related Topics

Disabling Password Recovery, on page 759

Password Recovery, on page 754

Information About Passwords and Privilege Levels

Default Password and Privilege Level Configuration

A simple way of providing terminal access control in your network is to use passwords and assign privilege levels. Password protection restricts access to a network or network device. Privilege levels define what commands users can enter after they have logged into a network device.

This table shows the default password and privilege level configuration.

Table 50: Default Password and Privilege Levels

Feature	Default Setting
Enable password and privilege level	No password is defined. The default is level 15 (privileged EXEC level). The password is not encrypted in the configuration file.
Enable secret password and privilege level	No password is defined. The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file.
Line password	No password is defined.

Additional Password Security

To provide an additional layer of security, particularly for passwords that cross the network or that are stored on a Trivial File Transfer Protocol (TFTP) server, you can use either the **enable password** or **enable secret** global configuration commands. Both commands accomplish the same thing; that is, you can establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level you specify.

We recommend that you use the **enable secret** command because it uses an improved encryption algorithm.

If you configure the **enable secret** command, it takes precedence over the **enable password** command; the two commands cannot be in effect simultaneously.

If you enable password encryption, it applies to all passwords including username passwords, authentication key passwords, the privileged command password, and console and virtual terminal line passwords.

Related Topics

Protecting Enable and Enable Secret Passwords with Encryption, on page 757
Example: Protecting Enable and Enable Secret Passwords with Encryption, on page 767

Password Recovery

By default, any end user with physical access to the switch can recover from a lost password by interrupting the boot process while the switch is powering on and then by entering a new password.

The password-recovery disable feature protects access to the switch password by disabling part of this functionality. When this feature is enabled, the end user can interrupt the boot process only by agreeing to set

the system back to the default configuration. With password recovery disabled, you can still interrupt the boot process and change the password, but the configuration file (config.text) and the VLAN database file (vlan.dat) are deleted.

If you disable password recovery, we recommend that you keep a backup copy of the configuration file on a secure server in case the end user interrupts the boot process and sets the system back to default values. Do not keep a backup copy of the configuration file on the switch. If the switch is operating in VTP transparent mode, we recommend that you also keep a backup copy of the VLAN database file on a secure server. When the switch is returned to the default system configuration, you can download the saved files to the switch by using the Xmodem protocol.

To re-enable password recovery, use the **service password-recovery** global configuration command.

Related Topics

Disabling Password Recovery, on page 759
Restrictions for Controlling Switch Access with Passwords and Privileges, on page 753

Terminal Line Telnet Configuration

When you power-up your switch for the first time, an automatic setup program runs to assign IP information and to create a default configuration for continued use. The setup program also prompts you to configure your switch for Telnet access through a password. If you did not configure this password during the setup program, you can configure it when you set a Telnet password for a terminal line.

Related Topics

Setting a Telnet Password for a Terminal Line, on page 760
Example: Setting a Telnet Password for a Terminal Line, on page 767

Username and Password Pairs

You can configure username and password pairs, which are locally stored on the switch. These pairs are assigned to lines or ports and authenticate each user before that user can access the switch. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.

Related Topics

Configuring Username and Password Pairs, on page 762

Privilege Levels

Cisco devices use privilege levels to provide password security for different levels of switch operation. By default, the Cisco IOS software operates in two modes (privilege levels) of password security: user EXEC (Level 1) and privileged EXEC (Level 15). You can configure up to 16 hierarchical levels of commands for each mode. By configuring multiple passwords, you can allow different sets of users to have access to specified commands.

Privilege Levels on Lines

Users can override the privilege level you set using the **privilege level** line configuration command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the **disable** command. If users know the password to a higher privilege level, they can use that password to enable the

higher privilege level. You might specify a high level or privilege level for your console line to restrict line usage.

For example, if you want many users to have access to the **clear line** command, you can assign it level 2 security and distribute the level 2 password fairly widely. But if you want more restricted access to the **configure** command, you can assign it level 3 security and distribute that password to a more restricted group of users.

Command Privilege Levels

When you set a command to a privilege level, all commands whose syntax is a subset of that command are also set to that level. For example, if you set the **show ip traffic** command to level 15, the **show** commands and **show ip** commands are automatically set to privilege level 15 unless you set them individually to different levels.

Related Topics

Setting the Privilege Level for a Command, on page 763
Example: Setting the Privilege Level for a Command, on page 767
Changing the Default Privilege Level for Lines, on page 765
Logging into and Exiting a Privilege Level, on page 766

How to Control Switch Access with Passwords and Privilege Levels

Setting or Changing a Static Enable Password

The enable password controls access to the privileged EXEC mode. Follow these steps to set or change a static enable password:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**enable password** *password* **Example:** `Switch(config)# enable password secret321`	Defines a new password or changes an existing password for access to privileged EXEC mode. By default, no password is defined.

	Command or Action	Purpose
		For *password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. It can contain the question mark (?) character if you precede the question mark with the key combination Crtl-v when you create the password; for example, to create the password abc?123, do this: **1.** Enter **abc**. **2.** Enter **Crtl-v**. **3.** Enter **?123**. When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter abc?123 at the password prompt.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Example: Setting or Changing a Static Enable Password, on page 767

Protecting Enable and Enable Secret Passwords with Encryption

Follow these steps to establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level you specify:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

Step 3	Use one of the following:
	• `enable password [level` *level*`]` {*password encryption-type encrypted-password*}
	• `enable secret [level` *level*`]` {*password encryption-type encrypted-password*}
	Example:
	`Switch(config)# enable password example102`
	or
	`Switch(config)# enable secret level 1 password secret123sample`
		• Defines a new password or changes an existing password for access to privileged EXEC mode.
		• Defines a secret password, which is saved using a nonreversible encryption method.
		• (Optional) For *level*, the range is from 0 to 15. Level 1 is normal user EXEC mode privileges. The default level is 15 (privileged EXEC mode privileges).
		• For *password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.
		• (Optional) For *encryption-type*, only type 5, a Cisco proprietary encryption algorithm, is available. If you specify an encryption type, you must provide an encrypted password—an encrypted password that you copy from another switch configuration.
		Note If you specify an encryption type and then enter a clear text password, you can not re-enter privileged EXEC mode. You cannot recover a lost encrypted password by any method.

	Command or Action	Purpose
Step 4	**service password-encryption** **Example:** `Switch(config)# service password-encryption`	(Optional) Encrypts the password when the password is defined or when the configuration is written. Encryption prevents the password from being readable in the configuration file.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Additional Password Security, on page 754
Example: Protecting Enable and Enable Secret Passwords with Encryption, on page 767

Disabling Password Recovery

Follow these steps to disable password recovery to protect the security of your switch:

Before you begin

If you disable password recovery, we recommend that you keep a backup copy of the configuration file on a secure server in case the end user interrupts the boot process and sets the system back to default values. Do not keep a backup copy of the configuration file on the switch. If the switch is operating in VTP transparent mode, we recommend that you also keep a backup copy of the VLAN database file on a secure server. When the switch is returned to the default system configuration, you can download the saved files to the switch by using the Xmodem protocol.

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Switch> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**system disable password recovery switch** {*all* | *<1-9>*} **Example:** `Switch(config)# system disable password recovery switch all`	Disables password recovery. • *all* - Sets the configuration on switches in stack. • *<1-9>* - Sets the configuration on the Switch Number selected. This setting is saved in an area of the flash memory that is accessible by the boot loader and the Cisco IOS image, but it is not part of the file system and is not accessible by any user.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

What to do next

To remove **disable password recovery**, use the **no system disable password recovery switch all** global configuration command.

Related Topics

Password Recovery, on page 754
Restrictions for Controlling Switch Access with Passwords and Privileges, on page 753

Setting a Telnet Password for a Terminal Line

Beginning in user EXEC mode, follow these steps to set a Telnet password for the connected terminal line:

Before you begin

- Attach a PC or workstation with emulation software to the switch console port, or attach a PC to the Ethernet management port.
- The default data characteristics of the console port are 9600, 8, 1, no parity. You might need to press the Return key several times to see the command-line prompt.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	**Note** If a password is required for access to privileged EXEC mode, you will be prompted for it. Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**line vty 0 15** **Example:** `Switch(config)# line vty 0 15`	Configures the number of Telnet sessions (lines), and enters line configuration mode. There are 16 possible sessions on a command-capable Switch. The 0 and 15 mean that you are configuring all 16 possible Telnet sessions.
Step 4	**password** *password* **Example:** `Switch(config-line)# password abcxyz543`	Sets a Telnet password for the line or lines. For *password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.
Step 5	**end** **Example:** `Switch(config-line)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Preventing Unauthorized Access, on page 751

Terminal Line Telnet Configuration, on page 755
Example: Setting a Telnet Password for a Terminal Line, on page 767

Configuring Username and Password Pairs

Follow these steps to configure username and password pairs:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

Step 3	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}
	Example:
	`Switch(config)# username adamsample privilege 1 password secret456`
	`Switch(config)# username 111111111111 mac attribute`
		Sets the username, privilege level, and password for each user.
		• For *name*, specify the user ID as one word or the MAC address. Spaces and quotation marks are not allowed.
		• You can configure a maximum of 12000 clients each, for both username and MAC filter.
		• (Optional) For *level*, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 1 gives user EXEC mode access.
		• For *encryption-type*, enter 0 to specify that an unencrypted password will follow. Enter 7 to specify that a hidden password will follow.
		• For *password*, specify the password the user must enter to gain access to the Switch. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command.

	Command or Action	Purpose

Step 4	Use one of the following:
	• **line console 0**
	• **line vty 0 15**
	Example:
	`Switch(config)# line console 0`
	or
	`Switch(config)# line vty 15`
		Enters line configuration mode, and configures the console port (line 0) or the VTY lines (line 0 to 15).

Step 5	**login local** **Example:** `Switch(config-line)# login local`	Enables local password checking at login time. Authentication is based on the username specified in Step 3.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Preventing Unauthorized Access, on page 751
Username and Password Pairs, on page 755

Setting the Privilege Level for a Command

Follow these steps to set the privilege level for a command:

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Switch> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**privilege** *mode* **level** *level command* **Example:** `Switch(config)# privilege exec level 14 configure`	Sets the privilege level for a command. • For *mode*, enter **configure** for global configuration mode, **exec** for EXEC mode, **interface** for interface configuration mode, or **line** for line configuration mode. • For *level*, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the **enable** password. • For *command*, specify the command to which you want to restrict access.
Step 4	**enable password level** *level password* **Example:** `Switch(config)# enable password level 14 SecretPswd14`	Specifies the password to enable the privilege level. • For *level*, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. • For *password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config`	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	`startup-config`	

Related Topics

Privilege Levels, on page 755
Example: Setting the Privilege Level for a Command, on page 767

Changing the Default Privilege Level for Lines

Follow these steps to change the default privilege level for the specified line:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**line vty** *line* **Example:** `Switch(config)# line vty 10`	Selects the virtual terminal line on which to restrict access.
Step 4	**privilege level** *level* **Example:** `Switch(config)# privilege level 15`	Changes the default privilege level for the line. For *level*, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the **enable** password.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:**	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	`Switch# copy running-config startup-config`	

What to do next

Users can override the privilege level you set using the **privilege level** line configuration command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the **disable** command. If users know the password to a higher privilege level, they can use that password to enable the higher privilege level. You might specify a high level or privilege level for your console line to restrict line usage.

Related Topics

Privilege Levels, on page 755

Logging into and Exiting a Privilege Level

Beginning in user EXEC mode, follow these steps to log into a specified privilege level and exit a specified privilege level.

Procedure

	Command or Action	Purpose
Step 1	**enable** *level* **Example:** `Switch> enable 15`	Logs in to a specified privilege level. Following the example, Level 15 is privileged EXEC mode. For *level*, the range is 0 to 15.
Step 2	**disable** *level* **Example:** `Switch# disable 1`	Exits to a specified privilege level. Following the example, Level 1 is user EXEC mode. For *level*, the range is 0 to 15.

Related Topics

Privilege Levels, on page 755

Monitoring Switch Access

Table 51: Commands for Displaying DHCP Information

show privilege	Displays the privilege level configuration.

Configuration Examples for Setting Passwords and Privilege Levels

Example: Setting or Changing a Static Enable Password

This example shows how to change the enable password to *l1u2c3k4y5*. The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

```
Switch(config)# enable password l1u2c3k4y5
```

Related Topics

Setting or Changing a Static Enable Password, on page 756

Example: Protecting Enable and Enable Secret Passwords with Encryption

This example shows how to configure the encrypted password *1FaD0$Xyti5Rkls3LoyxzS8* for privilege level 2:

```
Switch(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

Related Topics

Protecting Enable and Enable Secret Passwords with Encryption, on page 757
Additional Password Security, on page 754

Example: Setting a Telnet Password for a Terminal Line

This example shows how to set the Telnet password to *let45me67in89*:

```
Switch(config)# line vty 10
Switch(config-line)# password let45me67in89
```

Related Topics

Setting a Telnet Password for a Terminal Line, on page 760
Terminal Line Telnet Configuration, on page 755

Example: Setting the Privilege Level for a Command

This example shows how to set the **configure** command to privilege level 14 and define *SecretPswd14* as the password users must enter to use level 14 commands:

```
Switch(config)# privilege exec level 14 configure
Switch(config)# enable password level 14 SecretPswd14
```

Related Topics

Setting the Privilege Level for a Command, on page 763
Privilege Levels, on page 755

Additional References

Error Message Decoder

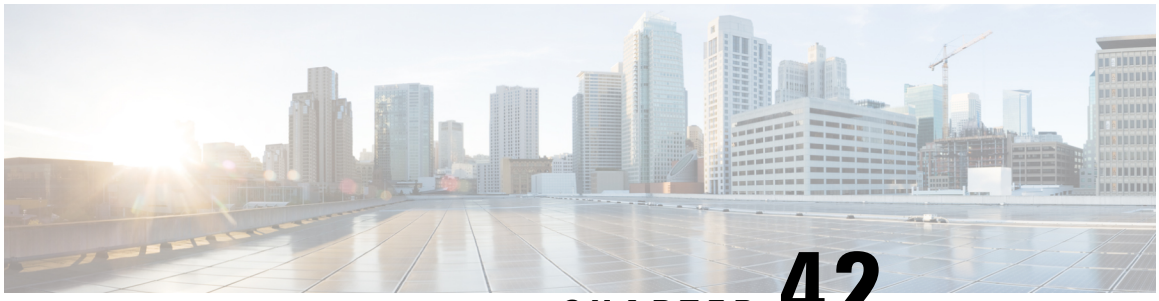
Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support



CHAPTER 42

Configuring TACACS+

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for TACACS+

The following are the prerequisites for set up and configuration of switch access with TACACS+ (must be performed in the order presented):

1. Configure the switches with the TACACS+ server addresses.
2. Set an authentication key.
3. Configure the key from Step 2 on the TACACS+ servers.
4. Enable authentication, authorization, and accounting (AAA).
5. Create a login authentication method list.
6. Apply the list to the terminal lines.
7. Create an authorization and accounting method list.

The following are the prerequisites for controlling switch access with TACACS+:

- You must have access to a configured TACACS+ server to configure TACACS+ features on your switch. Also, you must have access to TACACS+ services maintained in a database on a TACACS+ daemon typically running on a LINUX or Windows workstation.
- We recommend a redundant connection between a switch stack and the TACACS+ server. This is to help ensure that the TACACS+ server remains accessible in case one of the connected stack members is removed from the switch stack.
- You need a system running the TACACS+ daemon software to use TACACS+ on your switch.
- To use TACACS+, it must be enabled.
- Authorization must be enabled on the switch to be used.
- Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.
- To use any of the AAA commands listed in this section or elsewhere, you must first enable AAA with the **aaa new-model** command.
- At a minimum, you must identify the host or hosts maintaining the TACACS+ daemon and define the method lists for TACACS+ authentication. You can optionally define method lists for TACACS+ authorization and accounting.
- The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific port before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all ports except those that have a named method list explicitly defined. A defined method list overrides the default method list.
- Use TACACS+ for privileged EXEC access authorization if authentication was performed by using TACACS+.
- Use the local database if authentication was not performed by using TACACS+.

Related Topics

TACACS+ Overview, on page 771
TACACS+ Operation, on page 772
How to Configure Switch Access with TACACS+, on page 774
Method List, on page 773
Configuring TACACS+ Login Authentication, on page 776
TACACS+ Login Authentication, on page 773
Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services, on page 779
TACACS+ Authorization for Privileged EXEC Access and Network Services, on page 774

Information About TACACS+

TACACS+ and Switch Access

This section describes TACACS+. TACACS+ provides detailed accounting information and flexible administrative control over the authentication and authorization processes. It is facilitated through authentication, authorization, accounting (AAA) and can be enabled only through AAA commands.

Related Topics

Preventing Unauthorized Access, on page 751
Configuring the Switch for Local Authentication and Authorization, on page 837
SSH Servers, Integrated Clients, and Supported Versions, on page 843

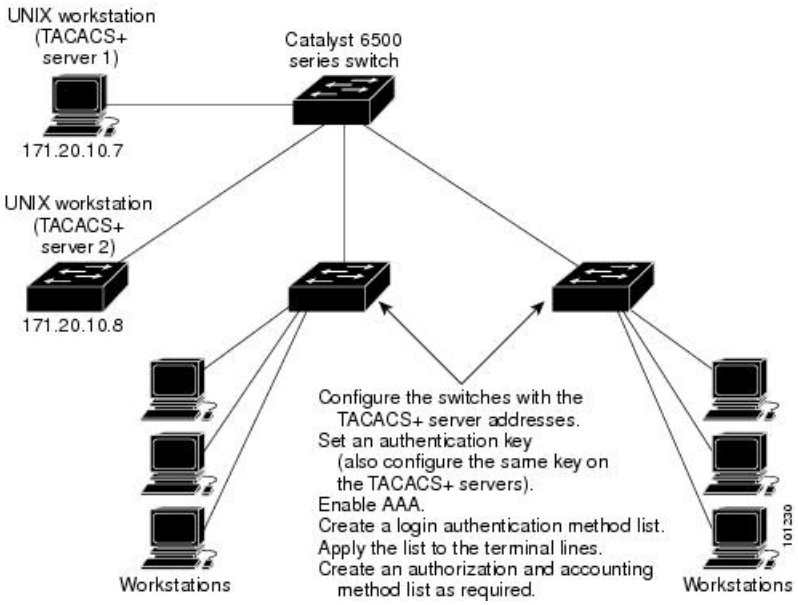
TACACS+ Overview

TACACS+ is a security application that provides centralized validation of users attempting to gain access to your switch.

TACACS+ provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service—authentication, authorization, and accounting—independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

The goal of TACACS+ is to provide a method for managing multiple network access points from a single management service. Your switch can be a network access server along with other Cisco routers and access servers.

Figure 41: Typical TACACS+ Network Configuration



TACACS+, administered through the AAA security services, can provide these services:

- Authentication—Provides complete control of authentication through login and password dialog, challenge and response, and messaging support.

  The authentication facility can conduct a dialog with the user (for example, after a username and password are provided, to challenge a user with several questions, such as home address, mother's maiden name, service type, and social security number). The TACACS+ authentication service can also send messages to user screens. For example, a message could notify users that their passwords must be changed because of the company's password aging policy.

- Authorization—Provides fine-grained control over user capabilities for the duration of the user's session, including but not limited to setting autocommands, access control, session duration, or protocol support. You can also enforce restrictions on what commands a user can execute with the TACACS+ authorization feature.

- Accounting—Collects and sends information used for billing, auditing, and reporting to the TACACS+ daemon. Network managers can use the accounting facility to track user activity for a security audit or to provide information for user billing. Accounting records include user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

The TACACS+ protocol provides authentication between the switch and the TACACS+ daemon, and it ensures confidentiality because all protocol exchanges between the switch and the TACACS+ daemon are encrypted.

Related Topics

Prerequisites for TACACS+, on page 769

TACACS+ Operation

When a user attempts a simple ASCII login by authenticating to a switch using TACACS+, this process occurs:

1. When the connection is established, the switch contacts the TACACS+ daemon to obtain a username prompt to show to the user. The user enters a username, and the switch then contacts the TACACS+ daemon to obtain a password prompt. The switch displays the password prompt to the user, the user enters a password, and the password is then sent to the TACACS+ daemon.

   TACACS+ allows a dialog between the daemon and the user until the daemon receives enough information to authenticate the user. The daemon prompts for a username and password combination, but can include other items, such as the user's mother's maiden name.

2. The switch eventually receives one of these responses from the TACACS+ daemon:

   - ACCEPT—The user is authenticated and service can begin. If the switch is configured to require authorization, authorization begins at this time.

   - REJECT—The user is not authenticated. The user can be denied access or is prompted to retry the login sequence, depending on the TACACS+ daemon.

   - ERROR—An error occurred at some time during authentication with the daemon or in the network connection between the daemon and the switch. If an ERROR response is received, the switch typically tries to use an alternative method for authenticating the user.

   - CONTINUE—The user is prompted for additional authentication information.

After authentication, the user undergoes an additional authorization phase if authorization has been enabled on the switch. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

3. If TACACS+ authorization is required, the TACACS+ daemon is again contacted, and it returns an ACCEPT or REJECT authorization response. If an ACCEPT response is returned, the response contains data in the form of attributes that direct the EXEC or NETWORK session for that user and the services that the user can access:
   - Telnet, Secure Shell (SSH), rlogin, or privileged EXEC services
   - Connection parameters, including the host or client IP address, access list, and user timeouts

Related Topics

Prerequisites for TACACS+, on page 769

Method List

A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a user. You can use method lists to designate one or more security protocols to be used, thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on users; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

Related Topics

How to Configure Switch Access with TACACS+, on page 774
Prerequisites for TACACS+, on page 769

TACACS+ Configuration Options

You can configure the switch to use a single server or AAA server groups to group existing server hosts for authentication. You can group servers to select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list and contains the list of IP addresses of the selected server hosts.

Related Topics

Identifying the TACACS+ Server Host and Setting the Authentication Key, on page 775

TACACS+ Login Authentication

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

Related Topics

Configuring TACACS+ Login Authentication, on page 776
Prerequisites for TACACS+, on page 769

TACACS+ Authorization for Privileged EXEC Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the switch uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

Related Topics

Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services, on page 779
Prerequisites for TACACS+, on page 769

TACACS+ Accounting

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the switch reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

Related Topics

Starting TACACS+ Accounting, on page 780

Default TACACS+ Configuration

TACACS+ and AAA are disabled by default.

To prevent a lapse in security, you cannot configure TACACS+ through a network management application. When enabled, TACACS+ can authenticate users accessing the switch through the CLI.

Note Although TACACS+ configuration is performed through the CLI, the TACACS+ server authenticates HTTP connections that have been configured with a privilege level of 15.

How to Configure Switch Access with TACACS+

This section describes how to configure your switch to support TACACS+.

Related Topics

Method List, on page 773
Prerequisites for TACACS+, on page 769

Identifying the TACACS+ Server Host and Setting the Authentication Key

Follow these steps to identify the TACACS+ server host and set the authentication key:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**tacacs server** *server-name* **Example:** `Switch(config)# tacacs server yourserver`	Identifies the IP host or hosts maintaining a TACACS+ server. Enter this command multiple times to create a list of preferred hosts. The software searches for hosts in the order in which you specify them. For *server-name*, specify the server name.
Step 4	**address** {**ipv4** | **ipv6**} *ip address* **Example:** `Switch(config-server-tacacs)# address ipv4 10.0.1.12`	Configures the IP address for the TACACS server.
Step 5	**exit** **Example:** `Switch(config-server-tacacs)# exit`	Exits the TACACS server mode and enters the global configuration mode.
Step 6	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables AAA.
Step 7	**aaa group server tacacs+** *group-name* **Example:** `Switch(config)# aaa group server tacacs+`	(Optional) Defines the AAA server-group with a group name. This command puts the Switch in a server group subconfiguration mode.

	Command or Action	Purpose
	`your_server_group`	
Step 8	**server** *ip-address* **Example:** `Switch(config)# server 10.1.2.3`	(Optional) Associates a particular TACACS+ server with the defined server group. Repeat this step for each TACACS+ server in the AAA server group. Each server in the group must be previously defined in Step 3.
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 10	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 11	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

TACACS+ Configuration Options, on page 773

Configuring TACACS+ Login Authentication

Follow these steps to configure TACACS+ login authentication:

Before you begin

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various ports.

Note To secure the switch for HTTP access by using AAA methods, you must configure the switch with the **ip http authentication aaa** global configuration command. Configuring AAA authentication does not secure the switch for HTTP access by using AAA methods.

For more information about the **ip http authentication** command, see the *Cisco IOS Security Command Reference, Release 12.4*.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables AAA.
Step 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Switch(config)# aaa authentication login default tacacs+ local`	Creates a login authentication method list. • To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports. • For *list-name*, specify a character string to name the list you are creating. • For *method1...*, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: • *enable*—Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the **enable** *password* global configuration command. • *group tacacs+*—Uses TACACS+ authentication. Before you can use this authentication method, you must configure the TACACS+ server.

	Command or Action	Purpose
		• *line* —Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the **password** *password* line configuration command. • *local*—Use the local username database for authentication. You must enter username information in the database. Use the **username** *password* global configuration command. • *local-case*—Use a case-sensitive local username database for authentication. You must enter username information in the database by using the **username** *name* **password** global configuration command. • *none*—Do not use any authentication for login.
Step 5	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*] **Example:** `Switch(config)# line 2 4`	Enters line configuration mode, and configures the lines to which you want to apply the authentication list.
Step 6	**login authentication** {**default** | *list-name*} **Example:** `Switch(config-line)# login authentication default`	Applies the authentication list to a line or set of lines. • If you specify **default**, use the default list created with the **aaa authentication login** command. • For *list-name*, specify the list created with the **aaa authentication login** command.
Step 7	**end** **Example:** `Switch(config-line)# end`	Returns to privileged EXEC mode.
Step 8	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.

	Command or Action	Purpose
Step 9	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

TACACS+ Login Authentication, on page 773
Prerequisites for TACACS+, on page 769

Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

You can use the **aaa authorization** global configuration command with the **tacacs+** keyword to set parameters that restrict a user's network access to privileged EXEC mode.

Note Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Follow these steps to specify TACACS+ authorization for privileged EXEC access and network services:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**aaa authorization network tacacs+** **Example:** `Switch(config)# aaa authorization network tacacs+`	Configures the switch for user TACACS+ authorization for all network-related service requests.

	Command or Action	Purpose
Step 4	**aaa authorization exec tacacs+** **Example:** `Switch(config)# aaa authorization exec tacacs+`	Configures the switch for user TACACS+ authorization if the user has privileged EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

TACACS+ Authorization for Privileged EXEC Access and Network Services, on page 774
Prerequisites for TACACS+, on page 769

Starting TACACS+ Accounting

Follow these steps to start TACACS+ Accounting:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters the global configuration mode.

	Command or Action	Purpose
	`Switch# configure terminal`	
Step 3	**aaa accounting network start-stop tacacs+** **Example:** `Switch(config)# aaa accounting network start-stop tacacs+`	Enables TACACS+ accounting for all network-related service requests.
Step 4	**aaa accounting exec start-stop tacacs+** **Example:** `Switch(config)# aaa accounting exec start-stop tacacs+`	Enables TACACS+ accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

To establish a session with a router if the AAA server is unreachable, use the **aaa accounting system guarantee-first** command. It guarantees system accounting as the first record, which is the default condition. In some situations, users might be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than 3 minutes.

To establish a console or Telnet session with the router if the AAA server is unreachable when the router reloads, use the **no aaa accounting system guarantee-first** command.

Related Topics

TACACS+ Accounting, on page 774

Establishing a Session with a Router if the AAA Server is Unreachable

To establishing a session with a router if the AAA server is unreachable, use the **aaa accounting system guarantee-first** command. It guarantees system accounting as the first record, which is the default condition. In some situations, users might be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than 3 minutes.

To establish a console or Telnet session with the router if the AAA server is unreachable when the router reloads, use the **no aaa accounting system guarantee-first** command.

Monitoring TACACS+

Table 52: Commands for Displaying TACACS+ Information

Command	Purpose
show tacacs	Displays TACACS+ server statistics.

Additional References for Configuring Secure Shell

Related Documents

Related Topic	Document Title
Configuring Identity Control policies and Identity Service templates for Session Aware networking.	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)
Configuring RADIUS, TACACS+, Secure Shell, 802.1X and AAA.	Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
None	

MIBs

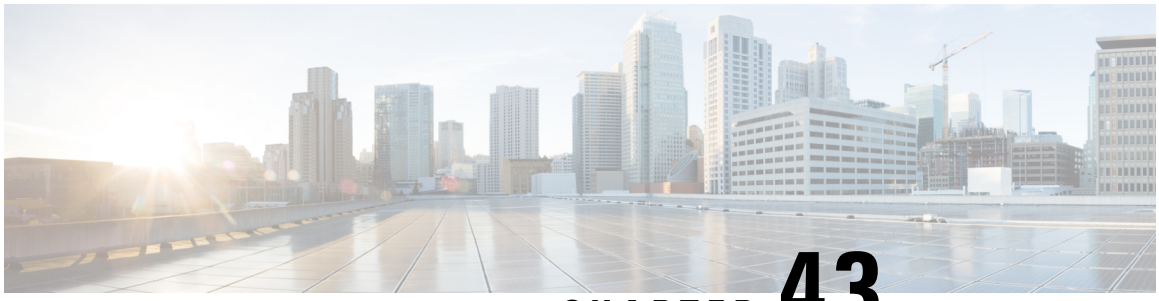
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for TACACS+

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.
Cisco IOS 12.2(54)SG Cisco IOS 15.2(1)E	The Per VRF for TACACS+ Servers feature allows per virtual route forwarding (per VRF) to be configured for authentication, authorization, and accounting (AAA) on TACACS+ servers. The following commands were introduced or modified: **ip tacacs source-interface**, **ip vrf forwarding (server-group)**, **server-private (TACACS+)**.



CHAPTER 43

Configuring RADIUS

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring RADIUS

This section lists the prerequisites for controlling Switch access with RADIUS.

General:

- RADIUS and Authentication, Authorization, and Accounting (AAA) must be enabled to use any of the configuration commands in this chapter.
- RADIUS is facilitated through AAA and can be enabled only through AAA commands.
- Use the **aaa new-model** global configuration command to enable AAA.
- Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication.

- Use **line** and **interface** commands to enable the defined method lists to be used.
- At a minimum, you must identify the host or hosts that run the RADIUS server software and define the method lists for RADIUS authentication. You can optionally define method lists for RADIUS authorization and accounting.
- You should have access to and should configure a RADIUS server before configuring RADIUS features on your Switch.
- The RADIUS host is normally a multiuser system running RADIUS server software from Cisco (Cisco Secure Access Control Server Version 3.0), Livingston, Merit, Microsoft, or another software provider. For more information, see the RADIUS server documentation.
- To use the Change-of-Authorization (CoA) interface, a session must already exist on the switch. CoA can be used to identify a session and enforce a disconnect request. The update affects only the specified session.
- A redundant connection between a switch stack and the RADIUS server is recommended. This is to help ensure that the RADIUS server remains accessible in case one of the connected stack members is removed from the switch stack.

For RADIUS operation:

- Users must first successfully complete RADIUS authentication before proceeding to RADIUS authorization, if it is enabled.

Related Topics

RADIUS and Switch Access, on page 787
RADIUS Operation, on page 788

Restrictions for Configuring RADIUS

This topic covers restrictions for controlling Switch access with RADIUS.

General:

- To prevent a lapse in security, you cannot configure RADIUS through a network management application.

RADIUS is not suitable in the following network security situations:

- Multiprotocol access environments. RADIUS does not support AppleTalk Remote Access (ARA), NetBIOS Frame Control Protocol (NBFCP), NetWare Asynchronous Services Interface (NASI), or X.25 PAD connections.
- Switch-to-switch or router-to-router situations. RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one device to a non-Cisco device if the non-Cisco device requires authentication.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

Related Topics

RADIUS Overview, on page 787

Information about RADIUS

RADIUS and Switch Access

This section describes how to enable and configure RADIUS. RADIUS provides detailed accounting information and flexible administrative control over the authentication and authorization processes.

Related Topics

Prerequisites for Configuring RADIUS, on page 785
Configuring the Switch for Local Authentication and Authorization, on page 837
SSH Servers, Integrated Clients, and Supported Versions, on page 843

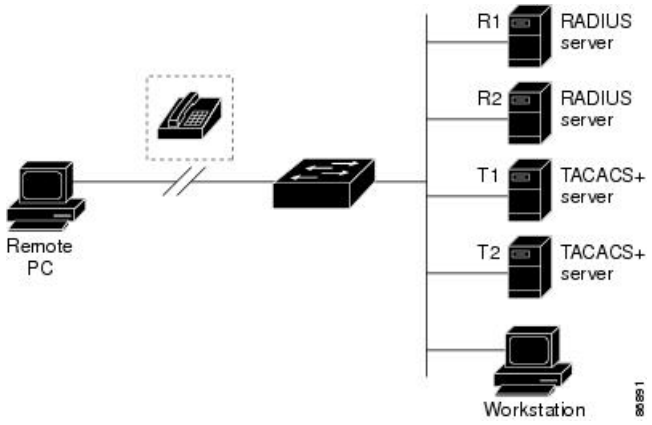
RADIUS Overview

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco routers and switches. Clients send authentication requests to a central RADIUS server, which contains all user authentication and network service access information.

Use RADIUS in these network environments that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.
- Turnkey network security environments in which applications support the RADIUS protocol, such as in an access environment that uses a *smart card* access control system. In one case, RADIUS has been used with Enigma's security cards to validates users and to grant access to network resources.
- Networks already using RADIUS. You can add a Cisco Switch containing a RADIUS client to the network. This might be the first step when you make a transition to a TACACS+ server. See Figure 2: Transitioning from RADIUS to TACACS+ Services below.
- Network in which the user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to the network through a protocol such as IEEE 802.1x. For more information about this protocol, see Chapter 11, "Configuring IEEE 802.1x Port-Based Authentication."
- Networks that require resource accounting. You can use RADIUS accounting independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, showing the amount of resources (such as time, packets, bytes, and so forth) used during the session. An Internet service provider might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

Figure 42: Transitioning from RADIUS to TACACS+ Services



Related Topics

Restrictions for Configuring RADIUS, on page 786

RADIUS Operation

When a user attempts to log in and authenticate to a Switch that is access controlled by a RADIUS server, these events occur:

1. The user is prompted to enter a username and password.
2. The username and encrypted password are sent over the network to the RADIUS server.
3. The user receives one of the following responses from the RADIUS server:
   - ACCEPT—The user is authenticated.
   - REJECT—The user is either not authenticated and is prompted to re-enter the username and password, or access is denied.
   - CHALLENGE—A challenge requires additional data from the user.
   - CHALLENGE PASSWORD—A response requests the user to select a new password.

   The ACCEPT or REJECT response is bundled with additional data that is used for privileged EXEC or network authorization. The additional data included with the ACCEPT or REJECT packets includes these items:

   - Telnet, SSH, rlogin, or privileged EXEC services
   - Connection parameters, including the host or client IP address, access list, and user timeouts

Related Topics

Prerequisites for Configuring RADIUS, on page 785

RADIUS Change of Authorization

The RADIUS Change of Authorization (CoA) provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated. When a policy changes for a user or user group in AAA, administrators can send RADIUS CoA packets from the AAA server such as a Cisco Secure Access Control Server (ACS) to reinitialize authentication and apply the new policy. This section provides an overview of the RADIUS interface including available primitives and how they are used during a CoA.

- Change-of-Authorization Requests
- CoA Request Response Code
- CoA Request Commands
- Session Reauthentication
- Stacking Guidelines for Session Termination

A standard RADIUS interface is typically used in a pulled model where the request originates from a network attached device and the response come from the queried servers. Catalyst switches support the RADIUS CoA extensions defined in RFC 5176 that are typically used in a pushed model and allow for the dynamic reconfiguring of sessions from external AAA or policy servers.

The switch supports these per-session CoA requests:

- Session reauthentication
- Session termination
- Session termination with port shutdown
- Session termination with port bounce

This feature is integrated with Cisco Secure Access Control Server (ACS) 5.1.

The RADIUS interface is enabled by default on Catalyst switches. However, some basic configuration is required for the following attributes:

- Security and Password—refer to the “Preventing Unauthorized Access to Your Switch” section in this guide.
- Accounting—refer to the “Starting RADIUS Accounting” section in the Configuring Switch-Based Authentication chapter in this guide.

Cisco IOS software supports the RADIUS CoA extensions defined in RFC 5176 that are typically used in a push model to allow the dynamic reconfiguring of sessions from external AAA or policy servers. Per-session CoA requests are supported for session identification, session termination, host reauthentication, port shutdown, and port bounce. This model comprises one request (CoA-Request) and two possible response codes:

- CoA acknowledgement (ACK) [CoA-ACK]
- CoA nonacknowledgement (NAK) [CoA-NAK]

The request is initiated from a CoA client (typically a AAA or policy server) and directed to the device that acts as a listener.

The table below shows the RADIUS CoA commands and vendor-specific attributes (VSAs) supported by Identity-Based Networking Services. All CoA commands must include the session identifier between the device and the CoA client.

Table 53: RADIUS CoA Commands Supported by Identity-Based Networking Services

CoA Command	Cisco VSA
Activate service	Cisco:Avpair="subscriber:command=activate-service" Cisco:Avpair="subscriber:service-name=<*service-name*>" Cisco:Avpair="subscriber:precedence=<*precedence-number*>" Cisco:Avpair="subscriber:activation-mode=replace-all"
Deactivate service	Cisco:Avpair="subscriber:command=deactivate-service" Cisco:Avpair="subscriber:service-name=<*service-name*>"
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"
Session query	Cisco:Avpair="subscriber:command=session-query"
Session reauthenticate	Cisco:Avpair="subscriber:command=reauthenticate" Cisco:Avpair="subscriber:reauthenticate-type=last" or Cisco:Avpair="subscriber:reauthenticate-type=rerun"
Session terminate	This is a standard disconnect request and does not require a VSA.
Interface template	Cisco:AVpair="interface-template-name=<*interfacetemplate*>"

Change-of-Authorization Requests

Change of Authorization (CoA) requests, as described in RFC 5176, are used in a push model to allow for session identification, host reauthentication, and session termination. The model is comprised of one request (CoA-Request) and two possible response codes:

- CoA acknowledgment (ACK) [CoA-ACK]
- CoA non-acknowledgment (NAK) [CoA-NAK]

The request is initiated from a CoA client (typically a RADIUS or policy server) and directed to the switch that acts as a listener.

RFC 5176 Compliance

The Disconnect Request message, which is also referred to as Packet of Disconnect (POD), is supported by the switch for session termination.

This table shows the IETF attributes are supported for this feature.

Table 54: Supported IETF Attributes

Attribute Number	Attribute Name
24	State
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

This table shows the possible values for the Error-Cause attribute.

Table 55: Error-Cause Values

Value	Explanation
201	Residual Session Context Removed
202	Invalid EAP Packet (Ignored)
401	Unsupported Attribute
402	Missing Attribute
403	NAS Identification Mismatch
404	Invalid Request
405	Unsupported Service
406	Unsupported Extension
407	Invalid Attribute Value
501	Administratively Prohibited
502	Request Not Routable (Proxy)
503	Session Context Not Found
504	Session Context Not Removable
505	Other Proxy Processing Error
506	Resources Unavailable
507	Request Initiated
508	Multiple Session Selection Unsupported

Preconditions

To use the CoA interface, a session must already exist on the switch. CoA can be used to identify a session and enforce a disconnect request. The update affects only the specified session.

CoA Request Response Code

The CoA Request response code can be used to convey a command to the switch.

The packet format for a CoA Request Response code as defined in RFC 5176 consists of the following fields: Code, Identifier, Length, Authenticator, and Attributes in the Type:Length:Value (TLV) format. The Attributes field is used to carry Cisco vendor-specific attributes (VSAs).

Related Topics

CoA Request Commands, on page 793

Session Identification

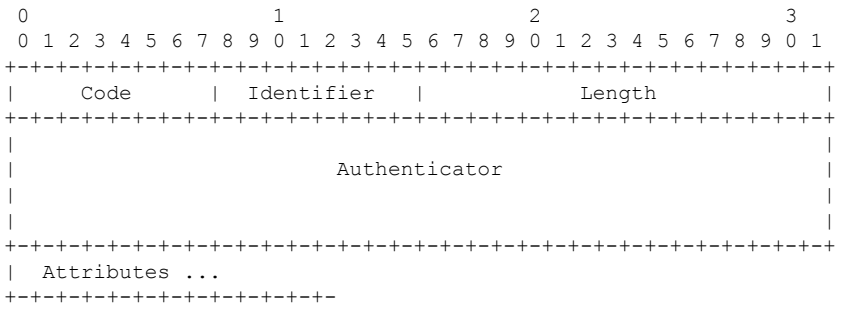
For disconnect and CoA requests targeted at a particular session, the switch locates the session based on one or more of the following attributes:

- Acct-Session-Id (IETF attribute #44)
- Audit-Session-Id (Cisco VSA)
- Calling-Station-Id (IETF attribute #31 which contains the host MAC address)
- IPv6 Attributes, which can be one of the following:
  - Framed-IPv6-Prefix (IETF attribute #97) and Framed-Interface-Id (IETF attribute #96), which together create a full IPv6 address per RFC 3162
  - Framed-IPv6-Address
- Plain IP Address (IETF attribute #8)

Unless all session identification attributes included in the CoA message match the session, the switch returns a Disconnect-NAK or CoA-NAK with the “Invalid Attribute Value” error-code attribute.

If more than one session identification attribute is included in the message, all the attributes must match the session or the switch returns a Disconnect- negative acknowledgment (NAK) or CoA-NAK with the error code “Invalid Attribute Value.”

The packet format for a CoA Request code as defined in RFC 5176 consists of the fields: Code, Identifier, Length, Authenticator, and Attributes in Type:Length:Value (TLV) format.



The attributes field is used to carry Cisco vendor-specific attributes (VSAs).

For CoA requests targeted at a particular enforcement policy, the device returns a CoA-NAK with the error code "Invalid Attribute Value" if any of the above session identification attributes are included in the message.

Related Topics

CoA Disconnect-Request, on page 794
CoA Request: Disable Host Port, on page 795
CoA Request: Bounce-Port, on page 795

CoA ACK Response Code

If the authorization state is changed successfully, a positive acknowledgment (ACK) is sent. The attributes returned within CoA ACK will vary based on the CoA Request and are discussed in individual CoA Commands.

CoA NAK Response Code

A negative acknowledgment (NAK) indicates a failure to change the authorization state and can include attributes that indicate the reason for the failure. Use **show** commands to verify a successful CoA.

CoA Request Commands

Table 56: CoA Commands Supported on the switch

Command [6]	Cisco VSA
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	This is a standard disconnect request that does not require a VSA.
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"

[6] All CoA commands must include the session identifier between the switch and the CoA client.

Related Topics

CoA Request Response Code, on page 792

Session Reauthentication

The AAA server typically generates a session reauthentication request when a host with an unknown identity or posture joins the network and is associated with a restricted access authorization profile (such as a guest VLAN). A reauthentication request allows the host to be placed in the appropriate authorization group when its credentials are known.

To initiate session authentication, the AAA server sends a standard CoA-Request message which contains a Cisco VSA in this form: *Cisco:Avpair="subscriber:command=reauthenticate"* and one or more session identification attributes.

The current session state determines the switch response to the message. If the session is currently authenticated by IEEE 802.1x, the switch responds by sending an EAPoL (Extensible Authentication Protocol over Lan) -RequestId message to the server.

If the session is currently authenticated by MAC authentication bypass (MAB), the switch sends an access-request to the server, passing the same identity attributes used for the initial successful authentication.

If session authentication is in progress when the switch receives the command, the switch terminates the process, and restarts the authentication sequence, starting with the method configured to be attempted first.

If the session is not yet authorized, or is authorized via guest VLAN, or critical VLAN, or similar policies, the reauthentication message restarts the access control methods, beginning with the method configured to be attempted first. The current authorization of the session is maintained until the reauthentication leads to a different authorization result.

Session Reauthentication in a Switch Stack

When a switch stack receives a session reauthentication message:

- It checkpoints the need for a re-authentication before returning an acknowledgment (ACK).
- It initiates reauthentication for the appropriate session.
- If authentication completes with either success or failure, the signal that triggered the reauthentication is removed from the stack member.
- If the stack master fails before authentication completes, reauthentication is initiated after stack master switch-over based on the original command (which is subsequently removed).
- If the stack master fails before sending an ACK, the new stack master treats the re-transmitted command as a new command.

Session Termination

There are three types of CoA requests that can trigger session termination. A CoA Disconnect-Request terminates the session, without disabling the host port. This command causes re-initialization of the authenticator state machine for the specified host, but does not restrict that host access to the network.

To restrict a host's access to the network, use a CoA Request with the Cisco:Avpair="subscriber:command=disable-host-port" VSA. This command is useful when a host is known to be causing problems on the network, and you need to immediately block network access for the host. When you want to restore network access on the port, re-enable it using a non-RADIUS mechanism.

When a device with no supplicant, such as a printer, needs to acquire a new IP address (for example, after a VLAN change), terminate the session on the host port with port-bounce (temporarily disable and then re-enable the port).

CoA Disconnect-Request

This command is a standard Disconnect-Request. If the session cannot be located, the switch returns a Disconnect-NAK message with the "Session Context Not Found" error-code attribute. If the session is located, the switch terminates the session. After the session has been completely removed, the switch returns a Disconnect-ACK.

If the switch fails-over to a standby switch before returning a Disconnect-ACK to the client, the process is repeated on the new active switch when the request is re-sent from the client. If the session is not found following re-sending, a Disconnect-ACK is sent with the "Session Context Not Found" error-code attribute.

Related Topics

Session Identification, on page 792

CoA Request: Disable Host Port

The RADIUS server CoA disable port command administratively shuts down the authentication port that is hosting a session, resulting in session termination. This command is useful when a host is known to cause problems on the network and network access needs to be immediately blocked for the host. To restore network access on the port, reenable it using a non-RADIUS mechanism. This command is carried in a standard CoA-Request message that has this new vendor-specific attribute (VSA):

Cisco:Avpair="subscriber:command=disable-host-port"

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the “Session Identification” section. If the session cannot be located, the switch returns a CoA-NAK message with the “Session Context Not Found” error-code attribute. If the session is located, the switch disables the hosting port and returns a CoA-ACK message.

If the switch fails before returning a CoA-ACK to the client, the process is repeated on the new active switch when the request is re-sent from the client. If the switch fails after returning a CoA-ACK message to the client but before the operation has completed, the operation is restarted on the new active switch.

Note A Disconnect-Request failure following command re-sending could be the result of either a successful session termination before change-over (if the Disconnect-ACK was not sent) or a session termination by other means (for example, a link failure) that occurred after the original command was issued and before the standby switch became active.

Related Topics

Session Identification, on page 792

CoA Request: Bounce-Port

A RADIUS server CoA bounce port sent from a RADIUS server can cause a link flap on an authentication port, which triggers DHCP renegotiation from one or more hosts connected to this port. This incident can occur when there is a VLAN change and the endpoint is a device (such as a printer) that does not have a mechanism to detect a change on this authentication port. The CoA bounce port is carried in a standard CoA-Request message that contains the following VSA:

Cisco:Avpair="subscriber:command=bounce-host-port"

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes. If the session cannot be located, the switch returns a CoA-NAK message with the “Session Context Not Found” error-code attribute. If the session is located, the switch disables the hosting port for a period of 10 seconds, re-enables it (port-bounce), and returns a CoA-ACK.

If the switch fails before returning a CoA-ACK to the client, the process is repeated on the new active switch when the request is re-sent from the client. If the switch fails after returning a CoA-ACK message to the client but before the operation has completed, the operation is re-started on the new active switch.

Related Topics

Session Identification, on page 792

Stacking Guidelines for Session Termination

No special handling is required for CoA Disconnect-Request messages in a switch stack.

Stacking Guidelines for CoA-Request Bounce-Port

Because the **bounce-port** command is targeted at a session, not a port, if the session is not found, the command cannot be executed.

When the Auth Manager command handler on the stack master receives a valid **bounce-port** command, it checkpoints the following information before returning a CoA-ACK message:

- the need for a port-bounce
- the port-id (found in the local session context)

The switch initiates a port-bounce (disables the port for 10 seconds, then re-enables it).

If the port-bounce is successful, the signal that triggered the port-bounce is removed from the standby stack master.

If the stack master fails before the port-bounce completes, a port-bounce is initiated after stack master change-over based on the original command (which is subsequently removed).

If the stack master fails before sending a CoA-ACK message, the new stack master treats the re-sent command as a new command.

Stacking Guidelines for CoA-Request Disable-Port

Because the **disable-port** command is targeted at a session, not a port, if the session is not found, the command cannot be executed.

When the Auth Manager command handler on the stack master receives a valid **disable-port** command, it verifies this information before returning a CoA-ACK message:

- the need for a port-disable
- the port-id (found in the local session context)

The switch attempts to disable the port.

If the port-disable operation is successful, the signal that triggered the port-disable is removed from the standby stack master.

If the stack master fails before the port-disable operation completes, the port is disabled after stack master change-over based on the original command (which is subsequently removed).

If the stack master fails before sending a CoA-ACK message, the new stack master treats the re-sent command as a new command.

Default RADIUS Configuration

RADIUS and AAA are disabled by default.

To prevent a lapse in security, you cannot configure RADIUS through a network management application. When enabled, RADIUS can authenticate users accessing the switch through the CLI.

RADIUS Server Host

Switch-to-RADIUS-server communication involves several components:

- Hostname or IP address

- Authentication destination port
- Accounting destination port
- Key string
- Timeout period
- Retransmission value

You identify RADIUS security servers by their hostname or IP address, hostname and specific UDP port numbers, or their IP address and specific UDP port numbers. The combination of the IP address and the UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address.

If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as a fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the %RADIUS-4-RADIUS_DEAD message appears, and then the switch tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order that they are configured.)

A RADIUS server and the switch use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the switch.

The timeout, retransmission, and encryption key values can be configured globally for all RADIUS servers, on a per-server basis, or in some combination of global and per-server settings.

Related Topics

Identifying the RADIUS Server Host, on page 810
Defining AAA Server Groups, on page 815
Configuring Settings for All RADIUS Servers, on page 820
Configuring RADIUS Login Authentication, on page 813

RADIUS Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various ports. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific port before any of the defined authentication methods are performed. The only exception is the default method list. The default method list is automatically applied to all ports except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

Related Topics

Configuring RADIUS Login Authentication, on page 813

AAA Server Groups

You can configure the switch to use AAA server groups to group existing server hosts for authentication. You select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list, which lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If you configure two different host entries on the same RADIUS server for the same service, (for example, accounting), the second configured host entry acts as a fail-over backup to the first one. If the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order in which they are configured.)

Related Topics

Defining AAA Server Groups, on page 815

AAA Authorization

AAA authorization limits the services available to a user. When AAA authorization is enabled, the switch uses information retrieved from the user's profile, which is in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

Related Topics

Configuring RADIUS Authorization for User Privileged Access and Network Services, on page 817

RADIUS Accounting

The AAA accounting feature tracks the services that users are using and the amount of network resources that they are consuming. When you enable AAA accounting, the switch reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. You can then analyze the data for network management, client billing, or auditing.

Related Topics

Starting RADIUS Accounting, on page 818

Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the switch and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named *cisco-avpair*. The value is a string with this format:

```
protocol : attribute sep value *
```

Protocol is a value of the Cisco protocol attribute for a particular type of authorization. *Attribute* and *value* are an appropriate attributevalue (AV) pair defined in the Cisco TACACS+ specification, and *sep* is = for mandatory attributes and is * for optional attributes. The full set of features available for TACACS+ authorization can then be used for RADIUS.

For example, the following AV pair causes Cisco's "multiple named IP address pools" feature to be activated during IP authorization (during PPP's Internet Protocol Control Protocol (IPCP) address assignment):

```
cisco-avpair= ”ip:addr-pool=first“
```

If you insert an "*", the AV pair "ip:addr-pool=first" becomes optional. Note that any AV pair can be made optional:

```
cisco-avpair= ”ip:addr-pool*first“
```

The following example shows how to cause a user logging in from a network access server to have immediate access to EXEC commands:

```
cisco-avpair= ”shell:priv-lvl=15“
```

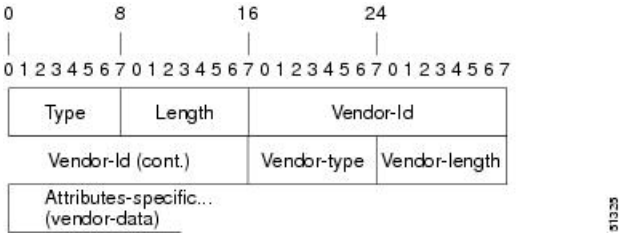
Other vendors have their own unique vendor-IDs, options, and associated VSAs. For more information about vendor-IDs and VSAs, see RFC 2138, "Remote Authentication Dial-In User Service (RADIUS)."

Attribute 26 contains the following three elements:

- Type
- Length
- String (also known as data)
  - Vendor-Id
  - Vendor-Type
  - Vendor-Length
  - Vendor-Data

The figure below shows the packet format for a VSA encapsulated "behind" attribute 26.

Figure 43: VSA Encapsulated Behind Attribute 26



Note It is up to the vendor to specify the format of their VSA. The Attribute-Specific field (also known as Vendor-Data) is dependent on the vendor's definition of that attribute.

The table below describes significant fields listed in the Vendor-Specific RADIUS IETF Attributes table (second table below), which lists supported vendor-specific RADIUS attributes (IETF attribute 26).

Table 57: Vendor-Specific Attributes Table Field Descriptions

Field	Description
Number	All attributes listed in the following table are extensions of IETF attribute 26.
Vendor-Specific Command Codes	A defined code used to identify a particular vendor. Code 9 defines Cisco VSAs, 311 defines Microsoft VSAs, and 529 defines Ascend VSAs.
Sub-Type Number	The attribute ID number. This number is much like the ID numbers of IETF attributes, except it is a “second layer” ID number encapsulated behind attribute 26.
Attribute	The ASCII string name of the attribute.
Description	Description of the attribute.

Table 58: Vendor-Specific RADIUS IETF Attributes

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
MS-CHAP Attributes				
26	311	1	MSCHAP-Response	Contains the response value provided by a PPP MS-CHAP user in response to the challenge. It is only used in Access-Request packets. This attribute is identical to the PPP CHAP Identifier. (RFC 2548
26	311	11	MSCHAP-Challenge	Contains the challenge sent by a network access server to an MS-CHAP user. It can be used in both Access-Request and Access-Challenge packets. (RFC 2548)
VPDN Attributes				
26	9	1	l2tp-cm-local-window-size	Specifies the maximum receive window size for L2TP control messages. This value is advertised to the peer during tunnel establishment.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	l2tp-drop-out-of-order	Respects sequence numbers on data packets by dropping those that are received out of order. This does not ensure that sequence numbers will be sent on data packets, just how to handle them if they are received.
26	9	1	l2tp-hello-interval	Specifies the number of seconds for the hello keepalive interval. Hello packets are sent when no data has been sent on a tunnel for the number of seconds configured here.
26	9	1	l2tp-hidden-avp	When enabled, sensitive AVPs in L2TP control messages are scrambled or hidden.
26	9	1	l2tp-nosession-timeout	Specifies the number of seconds that a tunnel will stay active with no sessions before timing out and shutting down.
26	9	1	tunnel-tos-reflect	Copies the IP ToS field from the IP header of each payload packet to the IP header of the tunnel packet for packets entering the tunnel at the LNS.
26	9	1	l2tp-tunnel-authen	If this attribute is set, it performs L2TP tunnel authentication.
26	9	1	l2tp-tunnel-password	Shared secret used for L2TP tunnel authentication and AVP hiding.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	l2tp-udp-checksum	This is an authorization attribute and defines whether L2TP should perform UDP checksums for data packets. Valid values are “yes” and “no.” The default is no.
Store and Forward Fax Attributes				
26	9	3	Fax-Account-Id-Origin	Indicates the account ID origin as defined by system administrator for the **mmoip aaa receive-id** or the **mmoip aaa send-id** commands.
26	9	4	Fax-Msg-Id=	Indicates a unique fax message identification number assigned by Store and Forward Fax.
26	9	5	Fax-Pages	Indicates the number of pages transmitted or received during this fax session. This page count includes cover pages.
26	9	6	Fax-Coverpage-Flag	Indicates whether or not a cover page was generated by the off-ramp gateway for this fax session. True indicates that a cover page was generated; false means that a cover page was not generated.
26	9	7	Fax-Modem-Time	Indicates the amount of time in seconds the modem sent fax data (x) and the amount of time in seconds of the total fax session (y), which includes both fax-mail and PSTN time, in the form x/y. For example, 10/15 means that the transfer time took 10 seconds, and the total fax session took 15 seconds.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	8	Fax-Connect-Speed	Indicates the modem speed at which this fax-mail was initially transmitted or received. Possible values are 1200, 4800, 9600, and 14400.
26	9	9	Fax-Recipient-Count	Indicates the number of recipients for this fax transmission. Until e-mail servers support Session mode, the number should be 1.
26	9	10	Fax-Process-Abort-Flag	Indicates that the fax session was aborted or successful. True means that the session was aborted; false means that the session was successful.
26	9	11	Fax-Dsn-Address	Indicates the address to which DSNs will be sent.
26	9	12	Fax-Dsn-Flag	Indicates whether or not DSN has been enabled. True indicates that DSN has been enabled; false means that DSN has not been enabled.
26	9	13	Fax-Mdn-Address	Indicates the address to which MDNs will be sent.
26	9	14	Fax-Mdn-Flag	Indicates whether or not message delivery notification (MDN) has been enabled. True indicates that MDN had been enabled; false means that MDN had not been enabled.
26	9	15	Fax-Auth-Status	Indicates whether or not authentication for this fax session was successful. Possible values for this field are success, failed, bypassed, or unknown.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	16	Email-Server-Address	Indicates the IP address of the e-mail server handling the on-ramp fax-mail message.
26	9	17	Email-Server-Ack-Flag	Indicates that the on-ramp gateway has received a positive acknowledgment from the e-mail server accepting the fax-mail message.
26	9	18	Gateway-Id	Indicates the name of the gateway that processed the fax session. The name appears in the following format: hostname.domain-name.
26	9	19	Call-Type	Describes the type of fax activity: fax receive or fax send.
26	9	20	Port-Used	Indicates the slot/port number of the Cisco AS5300 used to either transmit or receive this fax-mail.
26	9	21	Abort-Cause	If the fax session aborts, indicates the system component that signaled the abort. Examples of system components that could trigger an abort are FAP (Fax Application Process), TIFF (the TIFF reader or the TIFF writer), fax-mail client, fax-mail server, ESMTP client, or ESMTP server.
H323 Attributes				
26	9	23	Remote-Gateway-ID (h323-remote-address)	Indicates the IP address of the remote gateway.
26	9	24	Connection-ID (h323-conf-id)	Identifies the conference ID.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	25	Setup-Time (h323-setup-time)	Indicates the setup time for this connection in Coordinated Universal Time (UTC) formerly known as Greenwich Mean Time (GMT) and Zulu time.
26	9	26	Call-Origin (h323-call-origin)	Indicates the origin of the call relative to the gateway. Possible values are originating and terminating (answer).
26	9	27	Call-Type (h323-call-type)	Indicates call leg type. Possible values are **telephony** and **VoIP**.
26	9	28	Connect-Time (h323-connect-time)	Indicates the connection time for this call leg in UTC.
26	9	29	Disconnect-Time (h323-disconnect-time)	Indicates the time this call leg was disconnected in UTC.
26	9	30	Disconnect-Cause (h323-disconnect-cause)	Specifies the reason a connection was taken offline per Q.931 specification.
26	9	31	Voice-Quality (h323-voice-quality)	Specifies the impairment factor (ICPIF) affecting voice quality for a call.
26	9	33	Gateway-ID (h323-gw-id)	Indicates the name of the underlying gateway.
Large Scale Dialout Attributes				
26	9	1	callback-dialstring	Defines a dialing string to be used for callback.
26	9	1	data-service	No description available.
26	9	1	dial-number	Defines the number to dial.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	force-56	Determines whether the network access server uses only the 56 K portion of a channel, even when all 64 K appear to be available.
26	9	1	map-class	Allows the user profile to reference information configured in a map class of the same name on the network access server that dials out.
26	9	1	send-auth	Defines the protocol to use (PAP or CHAP) for username-password authentication following CLID authentication.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	send-name	PPP name authentication. To apply for PAP, do not configure the **ppp pap sent-name password** command on the interface. For PAP, "preauth:send-name" and "preauth:send-secret" will be used as the PAP username and PAP password for outbound authentication. For CHAP, "preauth:send-name" will be used not only for outbound authentication, but also for inbound authentication. For a CHAP inbound case, the NAS will use the name defined in "preauth:send-name" in the challenge packet to the caller box. **Note** The send-name attribute has changed over time: Initially, it performed the functions now provided by both the send-name and remote-name attributes. Because the remote-name attribute has been added, the send-name attribute is restricted to its current behavior.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	send-secret	PPP password authentication. The vendor-specific attributes (VSAs) “preauth:send-name” and “preauth:send-secret” will be used as the PAP username and PAP password for outbound authentication. For a CHAP outbound case, both “preauth:send-name” and “preauth:send-secret” will be used in the response packet.
26	9	1	remote-name	Provides the name of the remote host for use in large-scale dial-out. Dialer checks that the large-scale dial-out remote name matches the authenticated name, to protect against accidental user RADIUS misconfiguration. (For example, dialing a valid phone number but connecting to the wrong device.)
Miscellaneous Attributes				

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	2	Cisco-NAS-Port	Specifies additional vendor specific attribute (VSA) information for NAS-Port accounting. To specify additional NAS-Port information in the form an Attribute-Value Pair (AVPair) string, use the **radius-server vsa send** global configuration command. **Note** This VSA is typically used in Accounting, but may also be used in Authentication (Access-Request) packets.
26	9	1	min-links	Sets the minimum number of links for MLP.
26	9	1	proxyacl#<n>	Allows users to configure the downloadable user profiles (dynamic ACLs) by using the authentication proxy feature so that users can have the configured authorization to permit traffic going through the configured interfaces.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	spi	Carries the authentication information needed by the home agent to authenticate a mobile node during registration. The information is in the same syntax as the **ip mobile secure host <addr>** configuration command. Basically it contains the rest of the configuration command that follows that string, verbatim. It provides the Security Parameter Index (SPI), key, authentication algorithm, authentication mode, and replay protection timestamp range.

Related Topics

Configuring the Switch to Use Vendor-Specific RADIUS Attributes, on page 821

Vendor-Proprietary RADIUS Server Communication

Although an IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the switch and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco IOS software supports a subset of vendor-proprietary RADIUS attributes.

As mentioned earlier, to configure RADIUS (whether vendor-proprietary or IETF draft-compliant), you must specify the host running the RADIUS server daemon and the secret text string it shares with the switch. You specify the RADIUS host and secret text string by using the **radius server** global configuration commands.

Related Topics

Configuring the Switch for Vendor-Proprietary RADIUS Server Communication, on page 822

How to Configure RADIUS

Identifying the RADIUS Server Host

To apply these settings globally to all RADIUS servers communicating with the Switch, use the three unique global configuration commands: **radius-server timeout**, **radius-server retransmit**, and **key** *string*.

You can configure the Switch to use AAA server groups to group existing server hosts for authentication. For more information, see Related Topics below.

You also need to configure some settings on the RADIUS server. These settings include the IP address of the Switch and the key string to be shared by both the server and the Switch. For more information, see the RADIUS server documentation.

Follow these steps to configure per-server RADIUS server communication.

Before you begin

If you configure both global and per-server functions (timeout, retransmission, and key commands) on the switch, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands. For information on configuring these settings on all RADIUS servers, see Related Topics below.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**radius server** *server name* **Example:** `Switch(config)# radius server rsim`	
Step 4	**address** {**ipv4** | **ipv6**}*ip address*{ **auth-port** *port number* | **acct-port** *port number*} **Example:** `Switch(config-radius-server)# address ipv4 124.2.2.12 auth-port 1612`	(Optional) Specifies the RADIUS server parameters. For **auth-port** *port-number*, specify the UDP destination port for authentication requests. The default is 1645. The range is 0 to 65536. For **acct-port** *port-number*, specify the UDP destination port for authentication requests. The default is 1646.
Step 5	**key** *string* **Example:** `Switch(config-radius-server)# key rad123`	(Optional) For **key** *string*, specify the authentication and encryption key used between the Switch and the RADIUS daemon running on the RADIUS server.

	Command or Action	Purpose
		Note The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius server** command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
Step 6	**retransmit** *value* **Example:** `Switch(config-radius-server)# retransmit 10`	(Optional) Specifies the number of times a RADIUS request is resent when the server is not responding or responding slowly. The range is 1 to 100. This setting overrides the **radius-server retransmit** global configuration command setting.
Step 7	**timeout** *seconds* **Example:** `Switch(config-radius-server)# timeout 60`	(Optional) Specifies the time interval that the Switch waits for the RADIUS server to reply before sending a request again. The range is 1 to 1000. This setting overrides the **radius-server timeout** global configuration command setting.
Step 8	**exit** **Example:** `Switch(config-server-tacacs)# exit`	Exits the RADIUS server mode and enters the global configuration mode.
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 10	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 11	**copy running-config startup-config** **Example:** `Switch# copy running-config`	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	`startup-config`	

Related Topics

RADIUS Server Host, on page 796
Defining AAA Server Groups, on page 815
Configuring Settings for All RADIUS Servers, on page 820

Configuring RADIUS Login Authentication

Follow these steps to configure RADIUS login authentication:

Before you begin

To secure the switch for HTTP access by using AAA methods, you must configure the switch with the **ip http authentication aaa** global configuration command. Configuring AAA authentication does not secure the switch for HTTP access by using AAA methods.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables AAA.
Step 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Switch(config)# aaa authentication login default local`	Creates a login authentication method list. • To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports.

	Command or Action	Purpose
		• For *list-name*, specify a character string to name the list you are creating. • For *method1...*, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: • *enable*—Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the **enable** *password* global configuration command. • *group radius*—Use RADIUS authentication. Before you can use this authentication method, you must configure the RADIUS server. • *line*—Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the **password** *password* line configuration command. • *local*—Use the local username database for authentication. You must enter username information in the database. Use the **username** *name* **password** global configuration command. • *local-case*—Use a case-sensitive local username database for authentication. You must enter username information in the database by using the **username** *password* global configuration command. • *none*—Do not use any authentication for login.
Step 5	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*] **Example:**	Enters line configuration mode, and configure the lines to which you want to apply the authentication list.

	Command or Action	Purpose
	`Switch(config)# line 1 4`	
Step 6	**login authentication** {**default** | *list-name*} **Example:** `Switch(config)# login authentication default`	Applies the authentication list to a line or set of lines. • If you specify **default**, use the default list created with the **aaa authentication login** command. • For *list-name*, specify the list created with the **aaa authentication login** command.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 8	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 9	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

RADIUS Login Authentication, on page 797
RADIUS Server Host, on page 796

Defining AAA Server Groups

You use the **server** group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional **auth-port** and **acct-port** keywords.

Follow these steps to define AAA server groups:

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Switch> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**radius server** *name* **Example:** `Switch(config)# radius server ISE`	Specifies the name of the RADIUS server configuration for Protected Access Credential (PAC) provisioning and enters RADIUS server configuration mode. The switch also supports RADIUS for IPv6.
Step 4	**address** {**ipv4** | **ipv6**} {*ip-address* | *hostname*} **auth-port** *port-number* **acct-port** *port-number* **Example:** `Switch(config-radius-server)# address ipv4 10.1.1.1 auth-port 1645 acct-port 1646`	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.
Step 5	**key** *string* **Example:** `Switch(config-radius-server)# key cisco123`	Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server.
Step 6	**end** **Example:** `Switch(config-radius-server)# end`	Exits RADIUS server configuration mode and returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config`	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	`startup-config`	

Related Topics

Identifying the RADIUS Server Host, on page 810
RADIUS Server Host, on page 796
AAA Server Groups, on page 798

Configuring RADIUS Authorization for User Privileged Access and Network Services

Note Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Follow these steps to configure RADIUS authorization for user priviledged access and network services:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**aaa authorization network radius** **Example:** `Switch(config)# aaa authorization network radius`	Configures the switch for user RADIUS authorization for all network-related service requests.
Step 4	**aaa authorization exec radius** **Example:** `Switch(config)# aaa authorization exec radius`	Configures the switch for user RADIUS authorization if the user has privileged EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).

	Command or Action	Purpose
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

You can use the **aaa authorization** global configuration command with the **radius** keyword to set parameters that restrict a user's network access to privileged EXEC mode.

The **aaa authorization exec radius local** command sets these authorization parameters:

- Use RADIUS for privileged EXEC access authorization if authentication was performed by using RADIUS.
- Use the local database if authentication was not performed by using RADIUS.

Related Topics

AAA Authorization, on page 798

Starting RADIUS Accounting

Follow these steps to start RADIUS accounting:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**aaa accounting network start-stop radius** **Example:** `Switch(config)# aaa accounting network start-stop radius`	Enables RADIUS accounting for all network-related service requests.
Step 4	**aaa accounting exec start-stop radius** **Example:** `Switch(config)# aaa accounting exec start-stop radius`	Enables RADIUS accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

To establishing a session with a router if the AAA server is unreachable, use the **aaa accounting system guarantee-first** command. This command guarantees system accounting as the first record, which is the default condition. In some situations, users might be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than 3 minutes.

To establish a console or Telnet session with the router if the AAA server is unreachable when the router reloads, use the **no aaa accounting system guarantee-first** command.

Related Topics

RADIUS Accounting, on page 798

Establishing a Session with a Router if the AAA Server is Unreachable

The **aaa accounting system guarantee-first** command guarantees system accounting as the first record, which is the default condition. In some situations, users might be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than 3 minutes.

To establish a console or Telnet session with the router if the AAA server is unreachable when the router reloads, use the **no aaa accounting system guarantee-first** command.

Configuring Settings for All RADIUS Servers

Beginning in privileged EXEC mode, follow these steps to configure settings for all RADIUS servers:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

Step 2	**radius-server key** *string*
	Example:
	`Switch(config)# radius-server key your_server_key`
	`Switch(config)# key your_server_key`
		Specifies the shared secret text string used between the switch and all RADIUS servers.
		Note The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.

Step 3	**radius-server retransmit** *retries* **Example:** `Switch(config)# radius-server retransmit 5`	Specifies the number of times the switch sends each RADIUS request to the server before giving up. The default is 3; the range 1 to 1000.
Step 4	**radius-server timeout** *seconds* **Example:** `Switch(config)# radius-server timeout 3`	Specifies the number of seconds a switch waits for a reply to a RADIUS request before resending the request. The default is 5 seconds; the range is 1 to 1000.

	Command or Action	Purpose
Step 5	**radius-server deadtime** *minutes* **Example:** `Switch(config)# radius-server deadtime 0`	When a RADIUS server is not responding to authentication requests, this command specifies a time to stop the request on that server. This avoids the wait for the request to timeout before trying the next configured server. The default is 0; the range is 1 to 1440 minutes.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Identifying the RADIUS Server Host, on page 810
RADIUS Server Host, on page 796

Configuring the Switch to Use Vendor-Specific RADIUS Attributes

Follow these steps to configure the switch to use vendor-specific RADIUS attributes:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters the global configuration mode.

	Command or Action	Purpose
	`Switch# configure terminal`	
Step 3	**radius-server vsa send** [**accounting** | **authentication**] **Example:** `Switch(config)# radius-server vsa send accounting`	Enables the switch to recognize and use VSAs as defined by RADIUS IETF attribute 26. • (Optional) Use the **accounting** keyword to limit the set of recognized vendor-specific attributes to only accounting attributes. • (Optional) Use the **authentication** keyword to limit the set of recognized vendor-specific attributes to only authentication attributes. If you enter this command without keywords, both accounting and authentication vendor-specific attributes are used.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Vendor-Specific RADIUS Attributes, on page 798

Configuring the Switch for Vendor-Proprietary RADIUS Server Communication

Follow these steps to configure the switch to use vendor-proprietary RADIUS server communication:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**radius server** *server name* **Example:** `Switch(config)# radius server rsim`	Specifies the RADIUS server.
Step 4	**address** { **ipv4** | **ipv6** } *ip address* **Example:** `Switch(config-radius-server)# address ipv4 172.24.25.10`	(Optional) Specifies the IP address of the RADIUS server.
Step 5	**non-standard** **Example:** `Switch(config-radius-server)# non-standard`	Identifies that the RADIUS server using a vendor-proprietary implementation of RADIUS.
Step 6	**key** *string* **Example:** `Switch(config-radius-server)# key rad123`	Specifies the shared secret text string used between the switch and the vendor-proprietary RADIUS server. The switch and the RADIUS server use this text string to encrypt passwords and exchange responses.
Step 7	**exit** **Example:** `Switch(config-radius-server)# exit`	Exits the RADIUS server mode and enters the global configuration mode.
Step 8	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Switch(config)# end`	
Step 9	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 10	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Vendor-Proprietary RADIUS Server Communication, on page 810

Configuring CoA on the Switch

Follow these steps to configure CoA on a switch. This procedure is required.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables AAA.
Step 4	**aaa server radius dynamic-author** **Example:**	Configures the switch as an authentication, authorization, and accounting (AAA) server

	Command or Action	Purpose
	`Switch(config)# aaa server radius dynamic-author`	to facilitate interaction with an external policy server.
Step 5	**client** {*ip-address* | *name*} [**vrf** *vrfname*] [**server-key** *string*]	Enters dynamic authorization local server configuration mode and specifies a RADIUS client from which a device will accept CoA and disconnect requests.
Step 6	**server-key** [**0** | **7**] *string* **Example:** `Switch(config-sg-radius)# server-key your_server_key`	Configures the RADIUS key to be shared between a device and RADIUS clients.
Step 7	**port** *port-number* **Example:** `Switch(config-sg-radius)# port 25`	Specifies the port on which a device listens for RADIUS requests from configured RADIUS clients.
Step 8	**auth-type** {**any** | **all** | **session-key**} **Example:** `Switch(config-sg-radius)# auth-type any`	Specifies the type of authorization the switch uses for RADIUS clients. The client must match all the configured attributes for authorization.
Step 9	**ignore session-key**	(Optional) Configures the switch to ignore the session-key. For more information about the **ignore** command, see the *Cisco IOS Intelligent Services Gateway Command Reference* on Cisco.com.
Step 10	**ignore server-key** **Example:** `Switch(config-sg-radius)# ignore server-key`	(Optional) Configures the switch to ignore the server-key. For more information about the **ignore** command, see the *Cisco IOS Intelligent Services Gateway Command Reference* on Cisco.com.
Step 11	**authentication command bounce-port ignore** **Example:** `Switch(config-sg-radius)# authentication`	(Optional) Configures the switch to ignore a CoA request to temporarily disable the port hosting a session. The purpose of temporarily disabling the port is to trigger a DHCP renegotiation from the host when a VLAN

	Command or Action	Purpose
	`command bounce-port ignore`	change occurs and there is no supplicant on the endpoint to detect the change.
Step 12	**authentication command disable-port ignore** **Example:** `Switch(config-sg-radius)# authentication command disable-port ignore`	(Optional) Configures the switch to ignore a nonstandard command requesting that the port hosting a session be administratively shut down. Shutting down the port results in termination of the session. Use standard CLI or SNMP commands to re-enable the port.
Step 13	**end** **Example:** `Switch(config-sg-radius)# end`	Returns to privileged EXEC mode.
Step 14	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 15	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring RADIUS Server Load Balancing

This feature allows access and authentication requests to be evenly across all RADIUS servers in a server group. For more information, see the "RADIUS Server Load Balancing" chapter of the *Cisco IOS Security Configuration Guide, Release 12.4*.

Monitoring CoA Functionality

Table 59: Privileged EXEC show Commands

Command	Purpose
show aaa attributes protocol radius	Displays AAA attributes of RADIUS commands.

Table 60: Global Troubleshooting Commands

Command	Purpose
debug radius	Displays information for troubleshooting RADIUS.
debug aaa coa	Displays information for troubleshooting CoA processing.
debug aaa pod	Displays information for troubleshooting POD packets.
debug aaa subsys	Displays information for troubleshooting POD packets.
debug cmdhd [**detail** | **error** | **events**]	Displays information for troubleshooting command headers.

For detailed information about the fields in these displays, see the command reference for this release.

Configuration Examples for Controlling Switch Access with RADIUS

Examples: Identifying the RADIUS Server Host

This example shows how to configure one RADIUS server to be used for authentication and another to be used for accounting:

```
Switch(config)# radius server server1
Switch(config)# address ipv4 172.29.36.49 auth-port 1612
Switch(config)# key rad1
Switch(config)# address ipv4 172.20.36.50 acct-port 1618
Switch(config)# key rad2
```

Example: Using Two Different RADIUS Group Servers

In this example, the switch is configured to recognize two different RADIUS group servers (*group1* and *group2*). Group1 has two different host entries on the same RADIUS server configured for the same services. The second host entry acts as a fail-over backup to the first entry.

```
Switch(config)# radius server server1
Switch(config)# address 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# address 172.10.0.1 auth-port 1645 acct-port 1646
Switch(config)# aaa new-model
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```

Examples: Configuring the Switch to Use Vendor-Specific RADIUS Attributes

For example, this AV pair activates Cisco's *multiple named ip address pools* feature during IP authorization (during PPP IPCP address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

This example shows how to provide a user logging in from a switch with immediate access to privileged EXEC commands:

```
cisco-avpair= "shell:priv-lvl=15"
```

This example shows how to specify an authorized VLAN in the RADIUS server database:

```
cisco-avpair= "tunnel-type(#64)=VLAN(13)"
cisco-avpair= "tunnel-medium-type(#65)=802 media(6)"
cisco-avpair= "tunnel-private-group-id(#81)=vlanid"
```

This example shows how to apply an input ACL in ASCII format to an interface for the duration of this connection:

```
cisco-avpair= "ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0"
cisco-avpair= "ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any"
cisco-avpair= "mac:inacl#3=deny any any decnet-iv"
```

This example shows how to apply an output ACL in ASCII format to an interface for the duration of this connection:

```
cisco-avpair= "ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any"
```

Example: Configuring the Switch for Vendor-Proprietary RADIUS Server Communication

This example shows how to specify a vendor-proprietary RADIUS host and to use a secret key of *rad124* between the switch and the server:

```
Switch(config)# radius server server1
Switch(config)# address ipv4 172.20.30.15
Switch(config)# non-standard
Switch(config)# key rad124
```

Additional References for Configuring Secure Shell

Related Documents

Related Topic	Document Title
Configuring Identity Control policies and Identity Service templates for Session Aware networking.	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)
Configuring RADIUS, TACACS+, Secure Shell, 802.1X and AAA.	Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
None	

MIBs

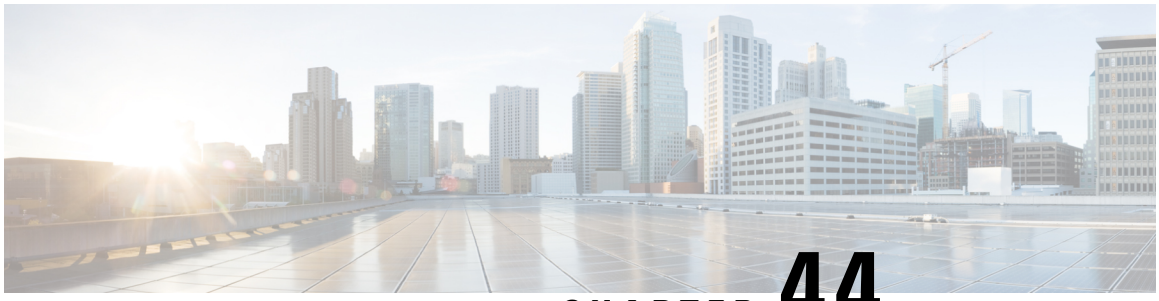
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for RADIUS

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.
Cisco IOS 15.2(1)E	The RADIUS Progress Codes feature adds additional progress codes to RADIUS attribute 196 (Ascend-Connect-Progress), which indicates a connection state before a call is disconnected through progress codes.
Cisco IOS 15.2(1)E	The Enhanced Test Command feature allows a named user profile to be created with calling line ID (CLID) or Dialed Number Identification Service (DNIS) attribute values. The CLID or DNIS attribute values can be associated with the RADIUS record that is sent with the user profile so that the RADIUS server can access CLID or DNIS attribute information for all incoming calls. The following commands were introduced or modified: **aaa attribute**, **aaa user profile**, and **test aaa group**



CHAPTER 44

Configuring Kerberos

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Controlling Switch Access with Kerberos

The following are the prerequisites for controlling switch access with Kerberos.

- So that remote users can authenticate to network services, you must configure the hosts and the KDC in the Kerberos realm to communicate and mutually authenticate users and network services. To do this, you must identify them to each other. You add entries for the hosts to the Kerberos database on the KDC and add KEYTAB files generated by the KDC to all hosts in the Kerberos realm. You also create entries for the users in the KDC database.
- A Kerberos server can be a switch that is configured as a network security server and that can authenticate users by using the Kerberos protocol.

When you add or create entries for the hosts and users, follow these guidelines:

- The Kerberos principal name *must* be in all lowercase characters.

- The Kerberos instance name *must* be in all lowercase characters.
- The Kerberos realm name *must* be in all uppercase characters.

Restrictions for Controlling Switch Access with Kerberos

The following lists any restrictions for controlling switch access with Kerberos.

Information about Kerberos

This section provides Kerberos information.

Kerberos and Switch Access

This section describes how to enable and configure the Kerberos security system, which authenticates requests for network resources by using a trusted third party.

Note In the Kerberos configuration examples, the trusted third party can be any switch that supports Kerberos, that is configured as a network security server, and that can authenticate users by using the Kerberos protocol.

Kerberos Overview

Kerberos is a secret-key network authentication protocol, which was developed at the Massachusetts Institute of Technology (MIT). It uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication and authenticates requests for network resources. Kerberos uses the concept of a trusted third party to perform secure verification of users and services. This trusted third party is called the *key distribution center* (KDC).

Kerberos verifies that users are who they claim to be and the network services that they use are what the services claim to be. To do this, a KDC or trusted Kerberos server issues tickets to users. These tickets, which have a limited life span, are stored in user credential caches. The Kerberos server uses the tickets instead of user names and passwords to authenticate users and network services.

Note A Kerberos server can be any switch that is configured as a network security server and that can authenticate users by using the Kerberos protocol.

The Kerberos credential scheme uses a process called *single logon*. This process authenticates a user once and then allows secure authentication (without encrypting another password) wherever that user credential is accepted.

This software release supports Kerberos 5, which allows organizations that are already using Kerberos 5 to use the same Kerberos authentication database on the KDC that they are already using on their other network hosts (such as UNIX servers and PCs).

Kerberos supports these network services:

- Telnet
- rlogin
- rsh

This table lists the common Kerberos-related terms and definitions.

Table 61: Kerberos Terms

Term	Definition
Authentication	A process by which a user or service identifies itself to another service. For example, a client can authenticate to a switch or a switch can authenticate to another switch.
Authorization	A means by which the switch identifies what privileges the user has in a network or on the switch and what actions the user can perform.
Credential	A general term that refers to authentication tickets, such as TGTs[7] and service credentials. Kerberos credentials verify the identity of a user or service. If a network service decides to trust the Kerberos server that issued a ticket, it can be used in place of re-entering a username and password. Credentials have a default life span of eight hours.
Instance	An authorization level label for Kerberos principals. Most Kerberos principals are of the form *user@REALM* (for example, smith@EXAMPLE.COM). A Kerberos principal with a Kerberos instance has the form *user/instance@REALM* (for example, smith/admin@EXAMPLE.COM). The Kerberos instance can be used to specify the authorization level for the user if authentication is successful. The server of each network service might implement and enforce the authorization mappings of Kerberos instances but is not required to do so. **Note** The Kerberos principal and instance names *must* be in all lowercase characters. **Note** The Kerberos realm name *must* be in all uppercase characters.
KDC[8]	Key distribution center that consists of a Kerberos server and database program that is running on a network host.
Kerberized	A term that describes applications and services that have been modified to support the Kerberos credential infrastructure.
Kerberos realm	A domain consisting of users, hosts, and network services that are registered to a Kerberos server. The Kerberos server is trusted to verify the identity of a user or network service to another user or network service. **Note** The Kerberos realm name *must* be in all uppercase characters.
Kerberos server	A daemon that is running on a network host. Users and network services register their identity with the Kerberos server. Network services query the Kerberos server to authenticate to other network services.

Term	Definition
KEYTAB[9]	A password that a network service shares with the KDC. In Kerberos 5 and later Kerberos versions, the network service authenticates an encrypted service credential by using the KEYTAB to decrypt it. In Kerberos versions earlier than Kerberos 5, KEYTAB is referred to as SRVTAB[10].
Principal	Also known as a Kerberos identity, this is who you are or what a service is according to the Kerberos server. **Note** The Kerberos principal name *must* be in all lowercase characters.
Service credential	A credential for a network service. When issued from the KDC, this credential is encrypted with the password shared by the network service and the KDC. The password is also shared with the user TGT.
SRVTAB	A password that a network service shares with the KDC. In Kerberos 5 or later Kerberos versions, SRVTAB is referred to as KEYTAB.
TGT	Ticket granting ticket that is a credential that the KDC issues to authenticated users. When users receive a TGT, they can authenticate to network services within the Kerberos realm represented by the KDC.

7 ticket granting ticket
8 key distribution center
9 key table
10 server table

Kerberos Operation

A Kerberos server can be a switch that is configured as a network security server and that can authenticate remote users by using the Kerberos protocol. Although you can customize Kerberos in a number of ways, remote users attempting to access network services must pass through three layers of security before they can access network services.

To authenticate to network services by using a switch as a Kerberos server, remote users must follow these steps:

Authenticating to a Boundary Switch

This section describes the first layer of security through which a remote user must pass. The user must first authenticate to the boundary switch. This process then occurs:

1. The user opens an un-Kerberized Telnet connection to the boundary switch.
2. The switch prompts the user for a username and password.
3. The switch requests a TGT from the KDC for this user.
4. The KDC sends an encrypted TGT that includes the user identity to the switch.
5. The switch attempts to decrypt the TGT by using the password that the user entered.
    - If the decryption is successful, the user is authenticated to the switch.

- If the decryption is not successful, the user repeats Step 2 either by re-entering the username and password (noting if Caps Lock or Num Lock is on or off) or by entering a different username and password.

A remote user who initiates a un-Kerberized Telnet session and authenticates to a boundary switch is inside the firewall, but the user must still authenticate directly to the KDC before getting access to the network services. The user must authenticate to the KDC because the TGT that the KDC issues is stored on the switch and cannot be used for additional authentication until the user logs on to the switch.

Obtaining a TGT from a KDC

This section describes the second layer of security through which a remote user must pass. The user must now authenticate to a KDC and obtain a TGT from the KDC to access network services.

For instructions about how to authenticate to a KDC, see the "Obtaining a TGT from a KDC" section in the "Security Server Protocols" chapter of the *Cisco IOS Security Configuration Guide, Release 12.4*.

Authenticating to Network Services

This section describes the third layer of security through which a remote user must pass. The user with a TGT must now authenticate to the network services in a Kerberos realm.

For instructions about how to authenticate to a network service, see the "Authenticating to Network Services" section in the "Security Server Protocols" chapter of the *Cisco IOS Security Configuration Guide, Release 12.4.*

How to Configure Kerberos

To set up a Kerberos-authenticated server-client system, follow these steps:

- Configure the KDC by using Kerberos commands.
- Configure the switch to use the Kerberos protocol.

Monitoring the Kerberos Configuration

To display the Kerberos configuration, use the following commands:

- **show running-config**
- **show kerberos creds**: Lists the credentials in a current user's credentials cache.
- **clear kerberos creds**: Destroys all credentials in a current user's credentials cache, including those forwarded.

Additional References

Related Documents

Related Topic	Document Title
Kerberos Commands	*Cisco IOS Security Command Reference*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

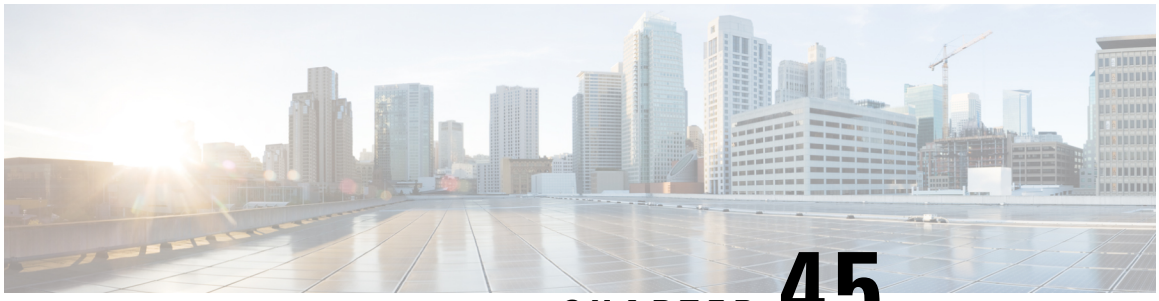
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Kerberos

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 45

Configuring Local Authentication and Authorization

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

How to Configure Local Authentication and Authorization

Configuring the Switch for Local Authentication and Authorization

You can configure AAA to operate without a server by setting the switch to implement AAA in local mode. The switch then handles authentication and authorization. No accounting is available in this configuration.

Note To secure the switch for HTTP access by using AAA methods, you must configure the switch with the **ip http authentication aaa** global configuration command. Configuring AAA authentication does not secure the switch for HTTP access by using AAA methods.

Follow these steps to configure AAA to operate without a server by setting the switch to implement AAA in local mode:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables AAA.
Step 4	**aaa authentication login default local** **Example:** `Switch(config)# aaa authentication login default local`	Sets the login authentication to use the local username database. The **default** keyword applies the local user database authentication to all ports.
Step 5	**aaa authorization exec default local** **Example:** `Switch(config)# aaa authorization exec default local`	Configures user AAA authorization, check the local database, and allow the user to run an EXEC shell.
Step 6	**aaa authorization network default local** **Example:** `Switch(config)# aaa authorization network default local`	Configures user AAA authorization for all network-related service requests.
Step 7	**username** *name* [**privilege** *level*] {**password** *encryption-type password*} **Example:** `Switch(config)# username your_user_name privilege 1 password 7 secret567`	Enters the local database, and establishes a username-based authentication system. Repeat this command for each user. • For *name*, specify the user ID as one word. Spaces and quotation marks are not allowed.

	Command or Action	Purpose
		• (Optional) For *level*, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 0 gives user EXEC mode access. • For *encryption-type*, enter 0 to specify that an unencrypted password follows. Enter 7 to specify that a hidden password follows. • For *password*, specify the password the user must enter to gain access to the switch. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command.
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 9	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 10	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

SSH Servers, Integrated Clients, and Supported Versions, on page 843
TACACS+ and Switch Access, on page 771
RADIUS and Switch Access, on page 787
Setting Up the Switch to Run SSH, on page 845
SSH Configuration Guidelines, on page 843

Monitoring Local Authentication and Authorization

To display Local Authentication and Authorization configuration, use the **show running-config** privileged EXEC command.

Additional References

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

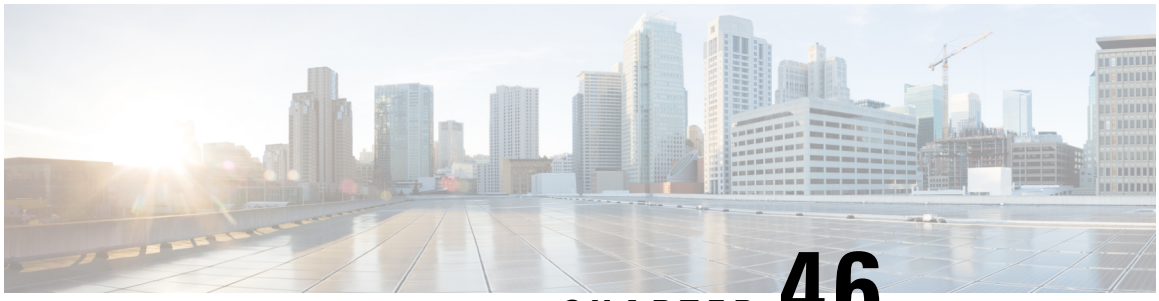
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Local Authentication and Authorization

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 46

Configuring Secure Shell (SSH)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Secure Shell

The following are the prerequisites for configuring the switch for secure shell (SSH):

- For SSH to work, the switch needs an Rivest, Shamir, and Adleman (RSA) public/private key pair. This is the same with Secure Copy Protocol (SCP), which relies on SSH for its secure transport.
- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.
- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.
- SCP relies on SSH for security.
- SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level.

- A user must have appropriate authorization to use SCP.
- A user who has appropriate authorization can use SCP to copy any file in the Cisco IOS File System (IFS) to and from a switch by using the **copy** command. An authorized administrator can also do this from a workstation.
- The Secure Shell (SSH) server requires an IPsec (Data Encryption Standard [DES] or 3DES) encryption software image; the SSH client requires an IPsec (DES or 3DES) encryption software image.)
- Configure a hostname and host domain for your device by using the **hostname** and **ip domain-name** commands in global configuration mode.

Related Topics

Secure Copy Protocol, on page 844

Restrictions for Configuring Secure Shell

The following are restrictions for configuring the Switch for secure shell.

- The switch supports Rivest, Shamir, and Adelman (RSA) authentication.
- SSH supports only the execution-shell application.
- The SSH server and the SSH client are supported only on Data Encryption Standard (DES) (56-bit) and 3DES (168-bit) data encryption software. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.
- The Switch supports the Advanced Encryption Standard (AES) encryption algorithm with a 128-bit key, 192-bit key, or 256-bit key. However, symmetric cipher AES to encrypt the keys is not supported.
- When using SCP, you cannot enter the password into the **copy** command. You must enter the password when prompted.
- The login banner is not supported in Secure Shell Version 1. It is supported in Secure Shell Version 2.
- The -l keyword and userid :{number} {ip-address} delimiter and arguments are mandatory when configuring the alternative method of Reverse SSH for console access.

Related Topics

Secure Copy Protocol, on page 844

Information About Configuring Secure Shell

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

SSH and Switch Access

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

SSH functions the same in IPv6 as in IPv4. For IPv6, SSH supports IPv6 addresses and enables secure, encrypted connections with remote IPv6 nodes over an IPv6 transport.

SSH Servers, Integrated Clients, and Supported Versions

The Secure Shell (SSH) Integrated Client feature is an application that runs over the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco device to make a secure, encrypted connection to another Cisco device or to any other device running the SSH server. This connection provides functionality similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for secure communication over an unsecured network.

The SSH server and SSH integrated client are applications that run on the switch. The SSH server works with the SSH client supported in this release and with non-Cisco SSH clients. The SSH client works with publicly and commercially available SSH servers. The SSH client supports the ciphers of Data Encryption Standard (DES), 3DES, and password authentication.

The switch supports an SSHv1 or an SSHv2 server.

The switch supports an SSHv1 client.

Note The SSH client functionality is available only when the SSH server is enabled.

User authentication is performed like that in the Telnet session to the device. SSH also supports the following user authentication methods:

- TACACS+
- RADIUS
- Local authentication and authorization

Related Topics

Configuring the Switch for Local Authentication and Authorization, on page 837
TACACS+ and Switch Access, on page 771
RADIUS and Switch Access, on page 787

SSH Configuration Guidelines

Follow these guidelines when configuring the switch as an SSH server or SSH client:

- An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.
- If the SSH server is running on a stack master and the stack master fails, the new stack master uses the RSA key pair generated by the previous stack master.
- If you get CLI error messages after entering the **crypto key generate rsa** global configuration command, an RSA key pair has not been generated. Reconfigure the hostname and domain, and then enter the **crypto key generate rsa** command. For more information, see Related Topics below.
- When generating the RSA key pair, the message No host name specified might appear. If it does, you must configure a hostname by using the **hostname** global configuration command.

- When generating the RSA key pair, the message No domain specified might appear. If it does, you must configure an IP domain name by using the **ip domain-name** global configuration command.
- When configuring the local authentication and authorization authentication method, make sure that AAA is disabled on the console.

Related Topics

Setting Up the Switch to Run SSH, on page 845
Configuring the Switch for Local Authentication and Authorization, on page 837

Secure Copy Protocol Overview

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying switch configurations or switch image files. SCP relies on Secure Shell (SSH), an application and a protocol that provides a secure replacement for the Berkeley r-tools.

For SSH to work, the switch needs an RSA public/private key pair. This is the same with SCP, which relies on SSH for its secure transport.

Because SSH also relies on AAA authentication, and SCP relies further on AAA authorization, correct configuration is necessary.

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.
- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.

Note When using SCP, you cannot enter the password into the copy command. You must enter the password when prompted.

Secure Copy Protocol

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying switch configurations or switch image files. The behavior of SCP is similar to that of remote copy (rcp), which comes from the Berkeley r-tools suite, except that SCP relies on SSH for security. SCP also requires that authentication, authorization, and accounting (AAA) authorization be configured so the switch can determine whether the user has the correct privilege level. To configure the Secure Copy feature, you should understand the SCP concepts.

Related Topics

Prerequisites for Configuring Secure Shell, on page 841
Restrictions for Configuring Secure Shell, on page 842

How to Configure SSH

Setting Up the Switch to Run SSH

Follow these steps to set up your Switch to run SSH:

Before you begin

Configure user authentication for local or remote access. This step is required. For more information, see Related Topics below.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**hostname** *hostname* **Example:** `Switch(config)# hostname your_hostname`	Configures a hostname and IP domain name for your Switch. **Note** Follow this procedure only if you are configuring the Switch as an SSH server.
Step 4	**ip domain-name** *domain_name* **Example:** `Switch(config)# ip domain-name your_domain`	Configures a host domain for your Switch.
Step 5	**crypto key generate rsa** **Example:** `Switch(config)# crypto key generate rsa`	Enables the SSH server for local and remote authentication on the Switch and generates an RSA key pair. Generating an RSA key pair for the Switch automatically enables SSH. We recommend that a minimum modulus size of 1024 bits.

	Command or Action	Purpose
		When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use. **Note** Follow this procedure only if you are configuring the Switch as an SSH server.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

SSH Configuration Guidelines, on page 843
Configuring the Switch for Local Authentication and Authorization, on page 837

Configuring the SSH Server

Follow these steps to configure the SSH server:

Note This procedure is only required if you are configuring the Switch as an SSH server.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Switch> enable`	
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip ssh version** [**1** | **2**] **Example:** `Switch(config)# ip ssh version 1`	(Optional) Configures the Switch to run SSH Version 1 or SSH Version 2. • **1**—Configure the Switch to run SSH Version 1. • **2**—Configure the Switch to run SSH Version 2. If you do not enter this command or do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.
Step 4	**ip ssh** {**timeout** *seconds* | **authentication-retries** *number*} **Example:** `Switch(config)# ip ssh timeout 90 authentication-retries 2`	Configures the SSH control parameters: • Specify the time-out value in seconds; the default is 120 seconds. The range is 0 to 120 seconds. This parameter applies to the SSH negotiation phase. After the connection is established, the Switch uses the default time-out values of the CLI-based sessions. By default, up to five simultaneous, encrypted SSH connections for multiple CLI-based sessions over the network are available (session 0 to session 4). After the execution shell starts, the CLI-based session time-out value returns to the default of 10 minutes. • Specify the number of times that a client can re-authenticate to the server. The default is 3; the range is 0 to 5. Repeat this step when configuring both parameters.
Step 5	Use one or both of the following: • `line vty`*line_number*[*ending_line_number*]	(Optional) Configures the virtual terminal line settings.

	Command or Action	Purpose

	• **transport input ssh**
	Example:
	`Switch(config)# line vty 1 10`
	or
	`Switch(config-line)# transport input ssh`
		• Enters line configuration mode to configure the virtual terminal line settings. For *line_number* and *ending_line_number*, specify a pair of lines. The range is 0 to 15.
		• Specifies that the Switch prevent non-SSH Telnet connections. This limits the router to only SSH connections.

Step 6	**end** **Example:** `Switch(config-line)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Monitoring the SSH Configuration and Status

This table displays the SSH server configuration and status.

Table 62: Commands for Displaying the SSH Server Configuration and Status

Command	Purpose
show ip ssh	Shows the version and configuration information for the SSH server.
show ssh	Shows the status of the SSH server.

Additional References for Configuring Secure Shell

Related Documents

Related Topic	Document Title
Configuring Identity Control policies and Identity Service templates for Session Aware networking.	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)
Configuring RADIUS, TACACS+, Secure Shell, 802.1X and AAA.	Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
None	

MIBs

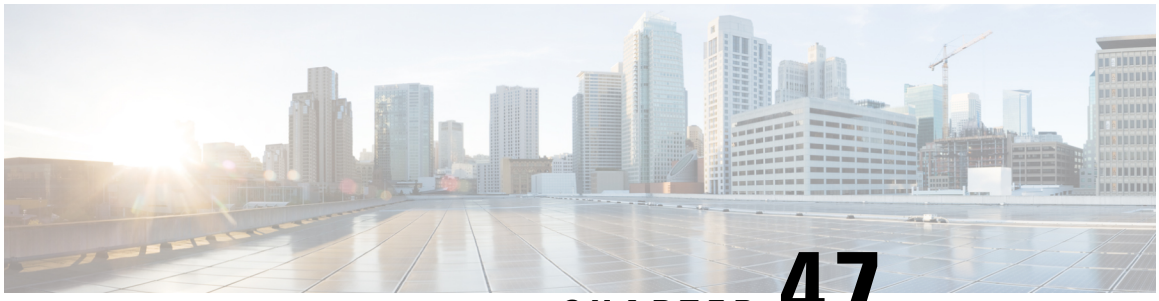
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Configuring Secure Shell

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.
Cisco IOS 15.2(1)E	The Reverse SSH Enhancements feature, which is supported for SSH Version 1 and 2, provides an alternative way to configure reverse Secure Shell (SSH) so that separate lines do not need to be configured for every terminal or auxiliary line on which SSH must be enabled. This feature also eliminates the rotary-group limitation. This feature was supported on CAT4500-X, CAT4500E-SUP6E, CAT4500E-SUP6L-E, CAT4500E-SUP7E, CAT4500E-SUP7L-E. The following command was introduced: **ssh**.



CHAPTER 47

Configuring Secure Socket Layer HTTP

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information about Secure Sockets Layer (SSL) HTTP

Secure HTTP Servers and Clients Overview

On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent over the Internet. HTTP with SSL encryption provides a secure connection to allow such functions as configuring a switch from a Web browser. Cisco's implementation of the secure HTTP server and secure HTTP client uses an implementation of SSL Version 3.0 with application-layer encryption. HTTP over SSL is abbreviated as HTTPS; the URL of a secure connection begins with https:// instead of http://.

Note SSL evolved into Transport Layer Security (TLS) in 1999, but is still used in this particular context.

The primary role of the HTTP secure server (the switch) is to listen for HTTPS requests on a designated port (the default HTTPS port is 443) and pass the request to the HTTP 1.1 Web server. The HTTP 1.1 server

processes requests and passes responses (pages) back to the HTTP secure server, which, in turn, responds to the original request.

The primary role of the HTTP secure client (the web browser) is to respond to Cisco IOS application requests for HTTPS User Agent services, perform HTTPS User Agent services for the application, and pass the response back to the application.

Note Beginning with Cisco IOS XE Denali 16.3.1, support for attaching IPv6 ACL to the HTTP server has been enabled. Prior to Cisco IOS XE Denali 16.3.1, only IPv4 ACL support was available for configuring the secure HTTP server. You can attach the preconfigured IPv6 and IPv4 ACLs to the HTTP server using the configuration CLI for the secure HTTP server.

Certificate Authority Trustpoints

Certificate authorities (CAs) manage certificate requests and issue certificates to participating network devices. These services provide centralized security key and certificate management for the participating devices. Specific CA servers are referred to as *trustpoints*.

When a connection attempt is made, the HTTPS server provides a secure connection by issuing a certified X.509v3 certificate, obtained from a specified CA trustpoint, to the client. The client (usually a Web browser), in turn, has a public key that allows it to authenticate the certificate.

For secure HTTP connections, we highly recommend that you configure a CA trustpoint. If a CA trustpoint is not configured for the device running the HTTPS server, the server certifies itself and generates the needed RSA key pair. Because a self-certified (self-signed) certificate does not provide adequate security, the connecting client generates a notification that the certificate is self-certified, and the user has the opportunity to accept or reject the connection. This option is useful for internal network topologies (such as testing).

If you do not configure a CA trustpoint, when you enable a secure HTTP connection, either a temporary or a persistent self-signed certificate for the secure HTTP server (or client) is automatically generated.

- If the switch is not configured with a hostname and a domain name, a temporary self-signed certificate is generated. If the switch reboots, any temporary self-signed certificate is lost, and a new temporary new self-signed certificate is assigned.
- If the switch has been configured with a host and domain name, a persistent self-signed certificate is generated. This certificate remains active if you reboot the switch or if you disable the secure HTTP server so that it will be there the next time you re-enable a secure HTTP connection.

Note The certificate authorities and trustpoints must be configured on each device individually. Copying them from other devices makes them invalid on the switch.

When a new certificate is enrolled, the new configuration change is not applied to the HTTPS server until the server is restarted. You can restart the server using either the CLI or by physical reboot. On restarting the server, the switch starts using the new certificate.

If a self-signed certificate has been generated, this information is included in the output of the **show running-config** privileged EXEC command. This is a partial sample output from that command displaying a self-signed certificate.

```
Switch# show running-config
Building configuration...

<output truncated>

crypto pki trustpoint TP-self-signed-3080755072
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3080755072
 revocation-check none
 rsakeypair TP-self-signed-3080755072
!
!
crypto ca certificate chain TP-self-signed-3080755072
 certificate self-signed 01
  3082029F 30820208 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  59312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33303830 37353530 37323126 30240609 2A864886 F70D0109
  02161743 45322D33 3535302D 31332E73 756D6D30 342D3335 3530301E 170D3933
  30333031 30303030 35395A17 0D323030 31303130 30303030 305A3059 312F302D

<output truncated>
```

You can remove this self-signed certificate by disabling the secure HTTP server and entering the **no crypto pki trustpoint TP-self-signed-30890755072** global configuration command. If you later re-enable a secure HTTP server, a new self-signed certificate is generated.

Note The values that follow *TP self-signed* depend on the serial number of the device.

You can use an optional command (**ip http secure-client-auth**) to allow the HTTPS server to request an X.509v3 certificate from the client. Authenticating the client provides more security than server authentication by itself.

For additional information on Certificate Authorities, see the "Configuring Certification Authority Interoperability" chapter in the *Cisco IOS Security Configuration Guide, Release 12.4*.

CipherSuites

A CipherSuite specifies the encryption algorithm and the digest algorithm to use on a SSL connection. When connecting to the HTTPS server, the client Web browser offers a list of supported CipherSuites, and the client and server negotiate the best encryption algorithm to use from those on the list that are supported by both. For example, Netscape Communicator 4.76 supports U.S. security with RSA Public Key Cryptography, MD2, MD5, RC2-CBC, RC4, DES-CBC, and DES-EDE3-CBC.

For the best possible encryption, you should use a client browser that supports 128-bit encryption, such as Microsoft Internet Explorer Version 5.5 (or later) or Netscape Communicator Version 4.76 (or later). The SSL_RSA_WITH_DES_CBC_SHA CipherSuite provides less security than the other CipherSuites, as it does not offer 128-bit encryption.

The more secure and more complex CipherSuites require slightly more processing time. This list defines the CipherSuites supported by the switch and ranks them from fastest to slowest in terms of router processing load (speed):

1. SSL_RSA_WITH_DES_CBC_SHA—RSA key exchange (RSA Public Key Cryptography) with DES-CBC for message encryption and SHA for message digest

2. SSL_RSA_WITH_NULL_SHA key exchange with NULL for message encryption and SHA for message digest (only for SSL 3.0).
3. SSL_RSA_WITH_NULL_MD5 key exchange with NULL for message encryption and MD5 for message digest (only for SSL 3.0).
4. SSL_RSA_WITH_RC4_128_MD5—RSA key exchange with RC4 128-bit encryption and MD5 for message digest
5. SSL_RSA_WITH_RC4_128_SHA—RSA key exchange with RC4 128-bit encryption and SHA for message digest
6. SSL_RSA_WITH_3DES_EDE_CBC_SHA—RSA key exchange with 3DES and DES-EDE3-CBC for message encryption and SHA for message digest
7. SSL_RSA_WITH_AES_128_CBC_SHA—RSA key exchange with AES 128-bit encryption and SHA for message digest (only for SSL 3.0).
8. SSL_RSA_WITH_AES_256_CBC_SHA—RSA key exchange with AES 256-bit encryption and SHA for message digest (only for SSL 3.0).
9. SSL_RSA_WITH_DHE_AES_128_CBC_SHA—RSA key exchange with AES 128-bit encryption and SHA for message digest (only for SSL 3.0).
10. SSL_RSA_WITH_DHE_AES_256_CBC_SHA—RSA key exchange with AES 256-bit encryption and SHA for message digest (only for SSL 3.0).

Note The latest versions of Chrome do not support the four original cipher suites, thus disallowing access to both web GUI and guest portals.

RSA (in conjunction with the specified encryption and digest algorithm combinations) is used for both key generation and authentication on SSL connections. This usage is independent of whether or not a CA trustpoint is configured.

Default SSL Configuration

The standard HTTP server is enabled.

SSL is enabled.

No CA trustpoints are configured.

No self-signed certificates are generated.

SSL Configuration Guidelines

When SSL is used in a switch cluster, the SSL session terminates at the cluster commander. Cluster member switches must run standard HTTP.

Before you configure a CA trustpoint, you should ensure that the system clock is set. If the clock is not set, the certificate is rejected due to an incorrect date.

In a switch stack, the SSL session terminates at the stack master.

How to Configure Secure HTTP Servers and Clients

Configuring a CA Trustpoint

For secure HTTP connections, we recommend that you configure an official CA trustpoint. A CA trustpoint is more secure than a self-signed certificate.

Beginning in privileged EXEC mode, follow these steps to configure a CA Trustpoint:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**hostname** *hostname* **Example:** `Switch(config)# hostname your_hostname`	Specifies the hostname of the switch (required only if you have not previously configured a hostname). The hostname is required for security keys and certificates.
Step 3	**ip domain-name** *domain-name* **Example:** `Switch(config)# ip domain-name your_domain`	Specifies the IP domain name of the switch (required only if you have not previously configured an IP domain name). The domain name is required for security keys and certificates.
Step 4	**crypto key generate rsa** **Example:** `Switch(config)# crypto key generate rsa`	(Optional) Generates an RSA key pair. RSA key pairs are required before you can obtain a certificate for the switch. RSA key pairs are generated automatically. You can use this command to regenerate the keys, if needed.
Step 5	**crypto ca trustpoint** *name* **Example:** `Switch(config)# crypto ca trustpoint your_trustpoint`	Specifies a local configuration name for the CA trustpoint and enter CA trustpoint configuration mode.
Step 6	**enrollment url** *url* **Example:**	Specifies the URL to which the switch should send certificate requests.

	Command or Action	Purpose
	`Switch(ca-trustpoint)# enrollment url http://your_server:80`	
Step 7	**enrollment http-proxy** *host-name port-number* **Example:** `Switch(ca-trustpoint)# enrollment http-proxy your_host 49`	(Optional) Configures the switch to obtain certificates from the CA through an HTTP proxy server. • For *host-name* , specify the proxy server used to get the CA. • For *port-number*, specify the port number used to access the CA.
Step 8	**crl query** *url* **Example:** `Switch(ca-trustpoint)# crl query ldap://your_host:49`	Configures the switch to request a certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.
Step 9	**primary** *name* **Example:** `Switch(ca-trustpoint)# primary your_trustpoint`	(Optional) Specifies that the trustpoint should be used as the primary (default) trustpoint for CA requests. • For *name*, specify the trustpoint that you just configured.
Step 10	**exit** **Example:** `Switch(ca-trustpoint)# exit`	Exits CA trustpoint configuration mode and return to global configuration mode.
Step 11	**crypto ca authentication** *name* **Example:** `Switch(config)# crypto ca authentication your_trustpoint`	Authenticates the CA by getting the public key of the CA. Use the same name used in Step 5.
Step 12	**crypto ca enroll** *name* **Example:** `Switch(config)# crypto ca enroll your_trustpoint`	Obtains the certificate from the specified CA trustpoint. This command requests a signed certificate for each RSA key pair.
Step 13	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Configuring the Secure HTTP Server

Beginning in privileged EXEC mode, follow these steps to configure a secure HTTP server:

Before you begin

If you are using a certificate authority for certification, you should use the previous procedure to configure the CA trustpoint on the switch before enabling the HTTP server. If you have not configured a CA trustpoint, a self-signed certificate is generated the first time that you enable the secure HTTP server. After you have configured the server, you can configure options (path, access list to apply, maximum number of connections, or timeout policy) that apply to both standard and secure HTTP servers.

To verify the secure HTTP connection by using a Web browser, enter https://*URL*, where the URL is the IP address or hostname of the server switch. If you configure a port other than the default port, you must also specify the port number after the URL. For example:

Note AES256_SHA2 is not supported.

```
https://209.165.129:1026
```

or

```
https://host.domain.com:1026
```

The existing **ip http access-class** *access-list-number* command for specifying the access-list(Only IPv4 ACLs) is going to be deprecated. You can still use this command to specify an access list to allow access to the HTTP server. Two new commands have been introduced to enable support for specifying IPv4 and IPv6 ACLs. These are **ip http access-class ipv4** *access-list-name* | *access-list-number* for specifying IPv4 ACLs and **ip http access-class ipv6** *access-list-name* for specifying IPv6 ACLs. We recommend using the new CLI to avoid receiving warning messages.

Note the following considerations for specifying access-lists:

- If you specify an access-list that does not exist, the configuration takes place but you receive the below warning message:

  ```
  ACL being attached does not exist, please configure it
  ```
- If you use the **ip http access-class** command for specifying an access-list for the HTTP server, the below warning message appears:

  ```
  This CLI will be deprecated soon, Please use new CLI ip http
  access-class ipv4/ipv6 <access-list-name>| <access-list-number>
  ```
- If you use **ip http access-class ipv4** *access-list-name* | *access-list-number* or **ip http access-class ipv6** *access-list-name* , and an access-list was already configured using **ip http access-class** , the below warning message appears:

  ```
  Removing ip http access-class <access-list-number>
  ```

ip http access-class *access-list-number* and **ip http access-class ipv4** *access-list-name* | *access-list-number* share the same functionality. Each command overrides the configuration of the previous command. The

following combinations between the configuration of the two commands explain the effect on the running configuration:

- If **ip http access-class** *access-list-number* is already configured and you try to configure using **ip http access-class ipv4** *access-list-number* command, the configuration of **ip http access-class** *access-list-number* will be removed and the configuration of **ip http access-class ipv4** *access-list-number* will be added to the running configuration.
- If **ip http access-class** *access-list-number* is already configured and you try to configure using **ip http access-class ipv4** *access-list-name* command, the configuration of **ip http access-class** *access-list-number* will be removed and the configuration of **ip http access-class ipv4** *access-list-name* will be added to the running configuration.
- If **ip http access-class ipv4** *access-list-number* is already configured and you try to configure using **ip http access-class** *access-list-name*, the configuration of **ip http access-class ipv4** *access-list-number* will be removed from configuration and the configuration of **ip http access-class** *access-list-name* will be added to the running configuration.
- If **ip http access-class ipv4** *access-list-name* is already configured and you try to configure using **ip http access-class** *access-list-number*, the configuration of **ip http access-class ipv4** *access-list-name* will be removed from the configuration and the configuration of **ip http access-class** *access-list-number* will be added to the running configuration.

Procedure

	Command or Action	Purpose

Step 1	**show ip http server status**
	Example:
	`Switch# show ip http server status`
		(Optional) Displays the status of the HTTP server to determine if the secure HTTP server feature is supported in the software. You should see one of these lines in the output:
		`HTTP secure server capability: Present`
		or
		`HTTP secure server capability: Not present`

Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ip http secure-server** **Example:** `Switch(config)# ip http secure-server`	Enables the HTTPS server if it has been disabled. The HTTPS server is enabled by default.

	Command or Action	Purpose
Step 4	**ip http secure-port** *port-number* **Example:** `Switch(config)# ip http secure-port 443`	(Optional) Specifies the port number to be used for the HTTPS server. The default port number is 443. Valid options are 443 or any number in the range 1025 to 65535.
Step 5	**ip http secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]} **Example:** `Switch(config)# ip http secure-ciphersuite rc4-128-md5`	(Optional) Specifies the CipherSuites (encryption algorithms) to be used for encryption over the HTTPS connection. If you do not have a reason to specify a particularly CipherSuite, you should allow the server and client to negotiate a CipherSuite that they both support. This is the default.
Step 6	**ip http secure-client-auth** **Example:** `Switch(config)# ip http secure-client-auth`	(Optional) Configures the HTTP server to request an X.509v3 certificate from the client for authentication during the connection process. The default is for the client to request a certificate from the server, but the server does not attempt to authenticate the client.
Step 7	**ip http secure-trustpoint** *name* **Example:** `Switch(config)# ip http secure-trustpoint your_trustpoint`	Specifies the CA trustpoint to use to get an X.509v3 security certificate and to authenticate the client certificate connection. **Note** Use of this command assumes you have already configured a CA trustpoint according to the previous procedure.
Step 8	**ip http path** *path-name* **Example:** `Switch(config)# ip http path /your_server:80`	(Optional) Sets a base HTTP path for HTML files. The path specifies the location of the HTTP server files on the local system (usually located in system flash memory).
Step 9	**ip http access-class** *access-list-number* **Example:** `Switch(config)# ip http access-class 2`	(Optional) Specifies an access list to use to allow access to the HTTP server.
Step 10	**ip http access-class** { **ipv4** {*access-list-number* | *access-list-name*} | **ipv6** {*access-list-name*} } **Example:**	(Optional)Specifies an access list to use to allow access to the HTTP server.

	Command or Action	Purpose
	`Switch(config)# ip http access-class ipv4 4`	
Step 11	**ip http max-connections** *value* **Example:** `Switch(config)# ip http max-connections 4`	(Optional) Sets the maximum number of concurrent connections that are allowed to the HTTP server. We recommend that the value be at least 10 and not less. This is required for the UI to function as expected.
Step 12	**ip http timeout-policy idle** *seconds* **life** *seconds* **requests** *value* **Example:** `Switch(config)# ip http timeout-policy idle 120 life 240 requests 1`	(Optional) Specifies how long a connection to the HTTP server can remain open under the defined circumstances: • **idle**—the maximum time period when no data is received or response data cannot be sent. The range is 1 to 600 seconds. The default is 180 seconds (3 minutes). • **life**—the maximum time period from the time that the connection is established. The range is 1 to 86400 seconds (24 hours). The default is 180 seconds. • **requests**—the maximum number of requests processed on a persistent connection. The maximum value is 86400. The default is 1.
Step 13	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Configuring the Secure HTTP Client

Beginning in privileged EXEC mode, follow these steps to configure a secure HTTP client:

Before you begin

The standard HTTP client and secure HTTP client are always enabled. A certificate authority is required for secure HTTP client certification. This procedure assumes that you have previously configured a CA trustpoint on the switch. If a CA trustpoint is not configured and the remote HTTPS server requires client authentication, connections to the secure HTTP client fail.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**ip http client secure-trustpoint** *name* **Example:** `Switch(config)# ip http client secure-trustpoint your_trustpoint`	(Optional) Specifies the CA trustpoint to be used if the remote HTTP server requests client authentication. Using this command assumes that you have already configured a CA trustpoint by using the previous procedure. The command is optional if client authentication is not needed or if a primary trustpoint has been configured.
Step 3	**ip http client secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]} **Example:** `Switch(config)# ip http client secure-ciphersuite rc4-128-md5`	(Optional) Specifies the CipherSuites (encryption algorithms) to be used for encryption over the HTTPS connection. If you do not have a reason to specify a particular CipherSuite, you should allow the server and client to negotiate a CipherSuite that they both support. This is the default.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Monitoring Secure HTTP Server and Client Status

To monitor the SSL secure server and client status, use the privileged EXEC commands in the following table.

Table 63: Commands for Displaying the SSL Secure Server and Client Status

Command	Purpose
show ip http client secure status	Shows the HTTP secure client configuration.
show ip http server secure status	Shows the HTTP secure server configuration.
show running-config	Shows the generated self-signed certificate for secure HTTP connections.

Additional References for Configuring Secure Shell

Related Documents

Related Topic	Document Title
Configuring Identity Control policies and Identity Service templates for Session Aware networking.	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)
Configuring RADIUS, TACACS+, Secure Shell, 802.1X and AAA.	Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
None	

MIBs

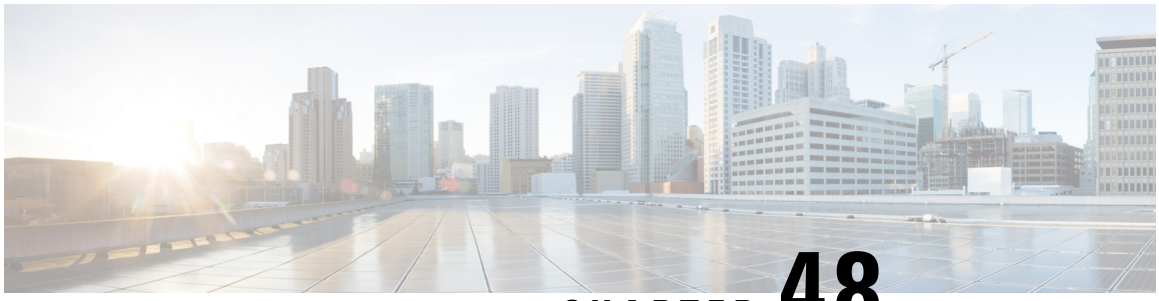
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Secure Socket Layer HTTP

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 48

Configuring IPv4 ACLs

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring IPv4 Access Control Lists

This section lists the prerequisites for configuring network security with access control lists (ACLs).

- On switches running the LAN base feature set, VLAN maps are not supported.

Restrictions for Configuring IPv4 Access Control Lists

General Network Security

The following are restrictions for configuring network security with ACLs:

- Not all commands that accept a numbered ACL accept a named ACL. ACLs for packet filters and route filters on interfaces can use a name. VLAN maps also accept a name.
- A standard ACL and an extended ACL cannot have the same name.
- Though visible in the command-line help strings, **appletalk** is not supported as a matching condition for the **deny** and **permit** MAC access-list configuration mode commands.
- ACL wildcard is not supported in downstream client policy.

IPv4 ACL Network Interfaces

The following restrictions apply to IPv4 ACLs to network interfaces:

- When controlling access to an interface, you can use a named or numbered ACL.
- If you apply an ACL to a Layer 2 interface that is a member of a VLAN, the Layer 2 (port) ACL takes precedence over an input Layer 3 ACL applied to the VLAN interface or a VLAN map applied to the VLAN.
- If you apply an ACL to a Layer 3 interface and routing is not enabled on the switch, the ACL only filters packets that are intended for the CPU, such as SNMP, Telnet, or web traffic.
- If the **preauth_ipv4_acl** ACL is configured to filter packets, the ACL is removed after authentication.
- You do not have to enable routing to apply ACLs to Layer 2 interfaces.

Note By default, the router sends Internet Control Message Protocol (ICMP) unreachable messages when a packet is denied by an access group on a Layer 3 interface. These access-group denied packets are not dropped in hardware but are bridged to the switch CPU so that it can generate the ICMP-unreachable message. They do not generate ICMP unreachable messages. ICMP unreachable messages can be disabled on router ACLs with the **no ip unreachables** interface command.

MAC ACLs on a Layer 2 Interface

After you create a MAC ACL, you can apply it to a Layer 2 interface to filter non-IP traffic coming in that interface. When you apply the MAC ACL, consider these guidelines:

- You can apply no more than one IP access list and one MAC access list to the same Layer 2 interface. The IP access list filters only IP packets, and the MAC access list filters non-IP packets.
- A Layer 2 interface can have only one MAC access list. If you apply a MAC access list to a Layer 2 interface that has a MAC ACL configured, the new ACL replaces the previously configured one.

Note The **mac access-group** interface configuration command is only valid when applied to a physical Layer 2 interface. You cannot use the command on EtherChannel port channels.

IP Access List Entry Sequence Numbering

- This feature does not support dynamic, reflexive, or firewall access lists.

Related Topics

Applying an IPv4 ACL to an Interface, on page 890
IPv4 ACL Interface Considerations, on page 879
Creating Named MAC Extended ACLs, on page 891
Applying a MAC ACL to a Layer 2 Interface, on page 893

Information about Network Security with ACLs

This chapter describes how to configure network security on the switch by using access control lists (ACLs), which in commands and tables are also referred to as access lists.

Cisco TrustSec and ACLs

Catalyst 3850 switches running the IP base or IP services feature set also support Cisco TrustSec Security Group Tag (SCT) Exchange Protocol (SXP). This feature supports security group access control lists (SGACLs), which define ACL policies for a group of devices instead of an IP address. The SXP control protocol allows tagging packets with SCTs without a hardware upgrade, and runs between access layer devices at the Cisco TrustSec domain edge and distribution layer devices within the Cisco TrustSec domain. Catalyst 3850 switches operate as access layer switches in the Cisco TrustSec network.

The sections on SXP define the capabilities supported on the Catalyst 3850 switches.

ACL Overview

Packet filtering can help limit network traffic and restrict network use by certain users or devices. ACLs filter traffic as it passes through a router or switch and permit or deny packets crossing specified interfaces or VLANs. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. One by one, it tests packets against the conditions in an access list. The first match decides whether the switch accepts or rejects the packets. Because the switch stops testing after the first match, the order of conditions in the list is critical. If no conditions match, the switch rejects the packet. If there are no restrictions, the switch forwards the packet; otherwise, the switch drops the packet. The switch can use ACLs on all packets it forwards, including packets bridged within a VLAN.

You configure access lists on a router or Layer 3 switch to provide basic security for your network. If you do not configure ACLs, all packets passing through the switch could be allowed onto all parts of the network. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at router interfaces. For example, you can allow e-mail traffic to be forwarded but not Telnet traffic. ACLs can be configured to block inbound traffic, outbound traffic, or both.

Access Control Entries

An ACL contains an ordered list of access control entries (ACEs). Each ACE specifies *permit* or *deny* and a set of conditions the packet must satisfy in order to match the ACE. The meaning of *permit* or *deny* depends on the context in which the ACL is used.

ACL Supported Types

The switch supports IP ACLs and Ethernet (MAC) ACLs:

- IP ACLs filter IPv4 traffic, including TCP, User Datagram Protocol (UDP), Internet Group Management Protocol (IGMP), and Internet Control Message Protocol (ICMP).
- Ethernet ACLs filter non-IP traffic.

This switch also supports quality of service (QoS) classification ACLs.

Supported ACLs

The switch supports three types of ACLs to filter traffic:

- Port ACLs access-control traffic entering a Layer 2 interface. You can apply port ACLs to a Layer 2 interface in each direction to each access list type — IPv4 and MAC.
- Router ACLs access-control routed traffic between VLANs and are applied to Layer 3 interfaces in a specific direction (inbound or outbound).
- VLAN ACLs or VLAN maps access-control all packets (bridged and routed). You can use VLAN maps to filter traffic between devices in the same VLAN. VLAN maps are configured to provide access control based on Layer 3 addresses for IPv4. Unsupported protocols are access-controlled through MAC addresses using Ethernet ACEs. After a VLAN map is applied to a VLAN, all packets (routed or bridged) entering the VLAN are checked against the VLAN map. Packets can either enter the VLAN through a switch port or through a routed port after being routed.

ACL Precedence

When VLAN maps, Port ACLs, and router ACLs are configured on the same switch, the filtering precedence, from greatest to least for ingress traffic is port ACL, VLAN map, and then router ACL. For egress traffic, the filtering precedence is router ACL, VLAN map, and then port ACL.

The following examples describe simple use cases:

- When both an input port ACL and a VLAN map are applied, incoming packets received on ports with a port ACL applied are filtered by the port ACL. Other packets are filtered by the VLAN map
- When an input router ACL and input port ACL exist in a switch virtual interface (SVI), incoming packets received on ports to which a port ACL is applied are filtered by the port ACL. Incoming routed IP packets received on other ports are filtered by the router ACL. Other packets are not filtered.
- When an output router ACL and input port ACL exist in an SVI, incoming packets received on the ports to which a port ACL is applied are filtered by the port ACL. Outgoing routed IP packets are filtered by the router ACL. Other packets are not filtered.
- When a VLAN map, input router ACL, and input port ACL exist in an SVI, incoming packets received on the ports to which a port ACL is applied are only filtered by the port ACL. Incoming routed IP packets received on other ports are filtered by both the VLAN map and the router ACL. Other packets are filtered only by the VLAN map.
- When a VLAN map, output router ACL, and input port ACL exist in an SVI, incoming packets received on the ports to which a port ACL is applied are only filtered by the port ACL. Outgoing routed IP packets

are filtered by both the VLAN map and the router ACL. Other packets are filtered only by the VLAN map.

Related Topics

Restrictions for Configuring IPv4 Access Control Lists, on page 865

Port ACLs

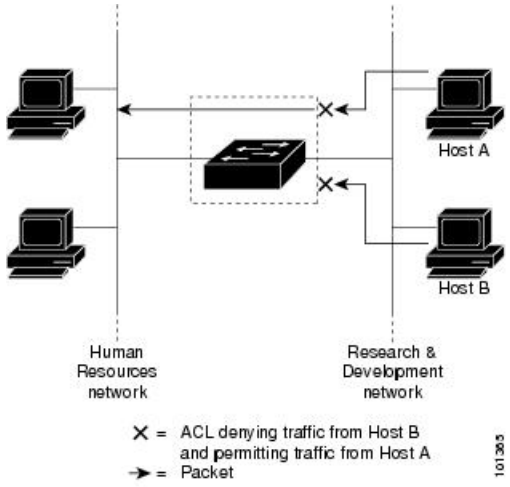
Port ACLs are ACLs that are applied to Layer 2 interfaces on a switch. Port ACLs are supported only on physical interfaces and not on EtherChannel interfaces. Port ACLs can be applied to the interface in outbound and inbound direction. The following access lists are supported:

- Standard IP access lists using source addresses
- Extended IP access lists using source and destination addresses and optional protocol type information
- MAC extended access lists using source and destination MAC addresses and optional protocol type information

The switch examines ACLs on an interface and permits or denies packet forwarding based on how the packet matches the entries in the ACL. In this way, ACLs control access to a network or to part of a network.

Figure 44: Using ACLs to Control Traffic in a Network

This is an example of using port ACLs to control access to a network when all workstations are in the same VLAN. ACLs applied at the Layer 2 input would allow Host A to access the Human Resources network, but prevent Host B from accessing the same network. Port ACLs can only be applied to Layer 2 interfaces in the



inbound direction.

When you apply a port ACL to a trunk port, the ACL filters traffic on all VLANs present on the trunk port. When you apply a port ACL to a port with voice VLAN, the ACL filters traffic on both data and voice VLANs.

With port ACLs, you can filter IP traffic by using IP access lists and non-IP traffic by using MAC addresses. You can filter both IP and non-IP traffic on the same Layer 2 interface by applying both an IP access list and a MAC access list to the interface.

Note You cannot apply more than one IP access list and one MAC access list to a Layer 2 interface. If an IP access list or MAC access list is already configured on a Layer 2 interface and you apply a new IP access list or MAC access list to the interface, the new ACL replaces the previously configured one.

Router ACLs

You can apply router ACLs on switch virtual interfaces (SVIs), which are Layer 3 interfaces to VLANs; on physical Layer 3 interfaces; and on Layer 3 EtherChannel interfaces. You apply router ACLs on interfaces for specific directions (inbound or outbound). You can apply one router ACL in each direction on an interface.

The switch supports these access lists for IPv4 traffic:

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses and optional protocol type information for matching operations.

As with port ACLs, the switch examines ACLs associated with features configured on a given interface. As packets enter the switch on an interface, ACLs associated with all inbound features configured on that interface are examined. After packets are routed and before they are forwarded to the next hop, all ACLs associated with outbound features configured on the egress interface are examined.

ACLs permit or deny packet forwarding based on how the packet matches the entries in the ACL, and can be used to control access to a network or to part of a network.

VLAN Maps

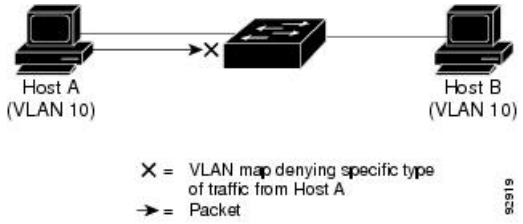
VLAN ACLs or VLAN maps are used to control network traffic within a VLAN. You can apply VLAN maps to all packets that are bridged within a VLAN in the switch or switch stack. VACLs are strictly for security packet filtering and for redirecting traffic to specific physical interfaces. VACLs are not defined by direction (ingress or egress).

All non-IP protocols are access-controlled through MAC addresses and Ethertype using MAC VLAN maps. (IP traffic is not access controlled by MAC VLAN maps.) You can enforce VLAN maps only on packets going through the switch; you cannot enforce VLAN maps on traffic between hosts on a hub or on another switch connected to this switch.

With VLAN maps, forwarding of packets is permitted or denied, based on the action specified in the map.

Figure 45: Using VLAN Maps to Control Traffic

This shows how a VLAN map is applied to prevent a specific type of traffic from Host A in VLAN 10 from being forwarded. You can apply only one VLAN map to a VLAN.



ACEs and Fragmented and Unfragmented Traffic

IP packets can be fragmented as they cross the network. When this happens, only the fragment containing the beginning of the packet contains the Layer 4 information, such as TCP or UDP port numbers, ICMP type and code, and so on. All other fragments are missing this information.

Some access control entries (ACEs) do not check Layer 4 information and therefore can be applied to all packet fragments. ACEs that do test Layer 4 information cannot be applied in the standard manner to most of the fragments in a fragmented IP packet. When the fragment contains no Layer 4 information and the ACE tests some Layer 4 information, the matching rules are modified:

- Permit ACEs that check the Layer 3 information in the fragment (including protocol type, such as TCP, UDP, and so on) are considered to match the fragment regardless of what the missing Layer 4 information might have been.

Note For TCP ACEs with L4 Ops, the fragmented packets will be dropped per RFC 1858.

- Deny ACEs that check Layer 4 information never match a fragment unless the fragment contains Layer 4 information.

ACEs and Fragmented and Unfragmented Traffic Examples

Consider access list 102, configured with these commands, applied to three fragmented packets:

```
Switch(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Switch(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Switch(config)# access-list 102 permit tcp any host 10.1.1.2
Switch(config)# access-list 102 deny tcp any any
```

Note In the first and second ACEs in the examples, the *eq* keyword after the destination address means to test for the TCP-destination-port well-known numbers equaling Simple Mail Transfer Protocol (SMTP) and Telnet, respectively.

- Packet A is a TCP packet from host 10.2.2.2., port 65000, going to host 10.1.1.1 on the SMTP port. If this packet is fragmented, the first fragment matches the first ACE (a permit) as if it were a complete packet because all Layer 4 information is present. The remaining fragments also match the first ACE, even though they do not contain the SMTP port information, because the first ACE only checks Layer 3 information when applied to fragments. The information in this example is that the packet is TCP and that the destination is 10.1.1.1.
- Packet B is from host 10.2.2.2, port 65001, going to host 10.1.1.2 on the Telnet port. If this packet is fragmented, the first fragment matches the second ACE (a deny) because all Layer 3 and Layer 4 information is present. The remaining fragments in the packet do not match the second ACE because they are missing Layer 4 information. Instead, they match the third ACE (a permit).

Because the first fragment was denied, host 10.1.1.2 cannot reassemble a complete packet, so packet B is effectively denied. However, the later fragments that are permitted will consume bandwidth on the network and resources of host 10.1.1.2 as it tries to reassemble the packet.

- Fragmented packet C is from host 10.2.2.2, port 65001, going to host 10.1.1.3, port ftp. If this packet is fragmented, the first fragment matches the fourth ACE (a deny). All other fragments also match the fourth ACE because that ACE does not check any Layer 4 information and because Layer 3 information in all fragments shows that they are being sent to host 10.1.1.3, and the earlier permit ACEs were checking different hosts.

ACLs and Switch Stacks

ACL support is the same for a switch stack as for a standalone switch. ACL configuration information is propagated to all switches in the stack. All switches in the stack, including the active switch, process the information and program their hardware.

Active Switch and ACL Functions

The active switch performs these ACL functions:

- It processes the ACL configuration and propagates the information to all stack members.
- It distributes the ACL information to any switch that joins the stack.
- If packets must be forwarded by software for any reason (for example, not enough hardware resources), the active switch forwards the packets only after applying ACLs on the packets.
- It programs its hardware with the ACL information it processes.

Stack Member and ACL Functions

Stack members perform these ACL functions:

- They receive the ACL information from the active switch and program their hardware.
- A stack member configured as a standby switch, performs the functions of the active switch in the event the active switch fails.

Active Switch Failure and ACLs

Both the active and standby switches have the ACL information. When the active switch fails, the standby takes over. The new active switch distributes the ACL information to all stack members.

Standard and Extended IPv4 ACLs

This section describes IP ACLs.

An ACL is a sequential collection of permit and deny conditions. One by one, the switch tests packets against the conditions in an access list. The first match determines whether the switch accepts or rejects the packet. Because the switch stops testing after the first match, the order of the conditions is critical. If no conditions match, the switch denies the packet.

The software supports these types of ACLs or access lists for IPv4:

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses for matching operations and optional protocol-type information for finer granularity of control.

IPv4 ACL Switch Unsupported Features

Configuring IPv4 ACLs on the switch is the same as configuring IPv4 ACLs on other Cisco switches and routers.

The following ACL-related features are not supported:

- Non-IP protocol ACLs
- IP accounting
- Reflexive ACLs and dynamic ACLs are not supported.

Access List Numbers

The number you use to denote your ACL shows the type of access list that you are creating.

This lists the access-list number and corresponding access list type and shows whether or not they are supported in the switch. The switch supports IPv4 standard and extended access lists, numbers 1 to 199 and 1300 to 2699.

Table 64: Access List Numbers

Access List Number	Type	Supported
1–99	IP standard access list	Yes
100–199	IP extended access list	Yes
200–299	Protocol type-code access list	No
300–399	DECnet access list	No
400–499	XNS standard access list	No
500–599	XNS extended access list	No
600–699	AppleTalk access list	No
700–799	48-bit MAC address access list	No
800–899	IPX standard access list	No
900–999	IPX extended access list	No
1000–1099	IPX SAP access list	No
1100–1199	Extended 48-bit MAC address access list	No
1200–1299	IPX summary address access list	No

Access List Number	Type	Supported
1300–1999	IP standard access list (expanded range)	Yes
2000–2699	IP extended access list (expanded range)	Yes

In addition to numbered standard and extended ACLs, you can also create standard and extended named IP ACLs by using the supported numbers. That is, the name of a standard IP ACL can be 1 to 99; the name of an extended IP ACL can be 100 to 199. The advantage of using named ACLs instead of numbered lists is that you can delete individual entries from a named list.

Numbered Standard IPv4 ACLs

When creating an ACL, remember that, by default, the end of the ACL contains an implicit deny statement for all packets that it did not find a match for before reaching the end. With standard access lists, if you omit the mask from an associated IP host address ACL specification, 0.0.0.0 is assumed to be the mask.

The switch always rewrites the order of standard access lists so that entries with **host** matches and entries with matches having a *don't care* mask of 0.0.0.0 are moved to the top of the list, above any entries with non-zero *don't care* masks. Therefore, in **show** command output and in the configuration file, the ACEs do not necessarily appear in the order in which they were entered.

After creating a numbered standard IPv4 ACL, you can apply it to VLANs, to terminal lines, or to interfaces.

Numbered Extended IPv4 ACLs

Although standard ACLs use only source addresses for matching, you can use extended ACL source and destination addresses for matching operations and optional protocol type information for finer granularity of control. When you are creating ACEs in numbered extended access lists, remember that after you create the ACL, any additions are placed at the end of the list. You cannot reorder the list or selectively add or remove ACEs from a numbered list.

The switch does not support dynamic or reflexive access lists. It also does not support filtering based on the type of service (ToS) minimize-monetary-cost bit.

Some protocols also have specific parameters and keywords that apply to that protocol.

You can define an extended TCP, UDP, ICMP, IGMP, or other IP ACL. The switch also supports these IP protocols:

Note ICMP echo-reply cannot be filtered. All other ICMP codes or types can be filtered.

These IP protocols are supported:

- Authentication Header Protocol (**ahp**)
- Encapsulation Security Payload (**esp**)
- Enhanced Interior Gateway Routing Protocol (**eigrp**)
- generic routing encapsulation (**gre**)

- Internet Control Message Protocol (**icmp**)
- Internet Group Management Protocol (**igmp**)
- any Interior Protocol (**ip**)
- IP in IP tunneling (**ipinip**)
- KA9Q NOS-compatible IP over IP tunneling (**nos**)
- Open Shortest Path First routing (**ospf**)
- Payload Compression Protocol (**pcp**)
- Protocol-Independent Multicast (**pim**)
- Transmission Control Protocol (**tcp**)
- User Datagram Protocol (**udp**)

Named IPv4 ACLs

You can identify IPv4 ACLs with an alphanumeric string (a name) rather than a number. You can use named ACLs to configure more IPv4 access lists in a router than if you were to use numbered access lists. If you identify your access list with a name rather than a number, the mode and command syntax are slightly different. However, not all commands that use IP access lists accept a named access list.

Note The name you give to a standard or extended ACL can also be a number in the supported range of access list numbers. That is, the name of a standard IP ACL can be 1 to 99 and . The advantage of using named ACLs instead of numbered lists is that you can delete individual entries from a named list.

Consider these guidelines before configuring named ACLs:

- Numbered ACLs are also available.
- A standard ACL and an extended ACL cannot have the same name.
- You can use standard or extended ACLs (named or numbered) in VLAN maps.

ACL Logging

The switch software can provide logging messages about packets permitted or denied by a standard IP access list. That is, any packet that matches the ACL causes an informational logging message about the packet to be sent to the console. The level of messages logged to the console is controlled by the **logging console** commands controlling the syslog messages.

Note ACL logging is only supported for RACL.

Note Because routing is done in hardware and logging is done in software, if a large number of packets match a *permit* or *deny* ACE containing a **log** keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

The first packet that triggers the ACL causes a logging message right away, and subsequent packets are collected over 5-minute intervals before they appear or logged. The logging message includes the access list number, whether the packet was permitted or denied, the source IP address of the packet, and the number of packets from that source permitted or denied in the prior 5-minute interval.

Note The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

Smart Logging

When smart logging is enabled on the switch and an ACL configured with smart logging is attached to a Layer 2 interface (port ACL), the contents of packets denied or permitted because of the ACL are also sent to a specified NetFlow collector.

Hardware and Software Treatment of IP ACLs

ACL processing is performed in hardware. If the hardware reaches its capacity to store ACL configurations, all packets on that interface are dropped.

Note If an ACL configuration cannot be implemented in hardware due to an out-of-resource condition on a switch or stack member, then only the traffic in that VLAN arriving on that switch is affected.

For router ACLs, other factors can cause packets to be sent to the CPU:

- Using the **log** keyword
- Generating ICMP unreachable messages

When you enter the **show ip access-lists** privileged EXEC command, the match count displayed does not account for packets that are access controlled in hardware. Use the **show platform acl counters hardware** privileged EXEC command to obtain some basic hardware ACL statistics for switched and routed packets.

Router ACLs function as follows:

- The hardware controls permit and deny actions of standard and extended ACLs (input and output) for security access control.
- If **log** has not been specified, the flows that match a *deny* statement in a security ACL are dropped by the hardware if *ip unreachables* is disabled. The flows matching a *permit* statement are switched in hardware.

- Adding the **log** keyword to an ACE in a router ACL causes a copy of the packet to be sent to the CPU for logging only. If the ACE is a *permit* statement, the packet is still switched and routed in hardware.

VLAN Map Configuration Guidelines

VLAN maps are the only way to control filtering within a VLAN. VLAN maps have no direction. To filter traffic in a specific direction by using a VLAN map, you need to include an ACL with specific source or destination addresses. If there is a match clause for that type of packet (IP or MAC) in the VLAN map, the default action is to drop the packet if the packet does not match any of the entries within the map. If there is no match clause for that type of packet, the default is to forward the packet.

The following are the VLAN map configuration guidelines:

- If there is no ACL configured to deny traffic on an interface and no VLAN map is configured, all traffic is permitted.
- Each VLAN map consists of a series of entries. The order of entries in an VLAN map is important. A packet that comes into the switch is tested against the first entry in the VLAN map. If it matches, the action specified for that part of the VLAN map is taken. If there is no match, the packet is tested against the next entry in the map.
- If the VLAN map has at least one match clause for the type of packet (IP or MAC) and the packet does not match any of these match clauses, the default is to drop the packet. If there is no match clause for that type of packet in the VLAN map, the default is to forward the packet.
- Logging is not supported for VLAN maps.
- When a switch has an IP access list or MAC access list applied to a Layer 2 interface, and you apply a VLAN map to a VLAN that the port belongs to, the port ACL takes precedence over the VLAN map.
- If a VLAN map configuration cannot be applied in hardware, all packets in that VLAN are dropped.

VLAN Maps with Router ACLs

To access control both bridged and routed traffic, you can use VLAN maps only or a combination of router ACLs and VLAN maps. You can define router ACLs on both input and output routed VLAN interfaces, and you can define a VLAN map to access control the bridged traffic.

If a packet flow matches a VLAN-map deny clause in the ACL, regardless of the router ACL configuration, the packet flow is denied.

Note When you use router ACLs with VLAN maps, packets that require logging on the router ACLs are not logged if they are denied by a VLAN map.

If the VLAN map has a match clause for the type of packet (IP or MAC) and the packet does not match the type, the default is to drop the packet. If there is no match clause in the VLAN map, and no action specified, the packet is forwarded if it does not match any VLAN map entry.

VLAN Maps and Router ACL Configuration Guidelines

These guidelines are for configurations where you need to have an router ACL and a VLAN map on the same VLAN. These guidelines do not apply to configurations where you are mapping router ACLs and VLAN maps on different VLANs.

If you must configure a router ACL and a VLAN map on the same VLAN, use these guidelines for both router ACL and VLAN map configuration:

- You can configure only one VLAN map and one router ACL in each direction (input/output) on a VLAN interface.
- Whenever possible, try to write the ACL with all entries having a single action except for the final, default action of the other type. That is, write the ACL using one of these two forms:

  permit... permit... permit... deny ip any any

  or

  deny... deny... deny... permit ip any any
- To define multiple actions in an ACL (permit, deny), group each action type together to reduce the number of entries.
- Avoid including Layer 4 information in an ACL; adding this information complicates the merging process. The best merge results are obtained if the ACLs are filtered based on IP addresses (source and destination) and not on the full flow (source IP address, destination IP address, protocol, and protocol ports). It is also helpful to use *don't care* bits in the IP address, whenever possible.

  If you need to specify the full-flow mode and the ACL contains both IP ACEs and TCP/UDP/ICMP ACEs with Layer 4 information, put the Layer 4 ACEs at the end of the list. This gives priority to the filtering of traffic based on IP addresses.

Time Ranges for ACLs

You can selectively apply extended ACLs based on the time of day and the week by using the **time-range** global configuration command. First, define a time-range name and set the times and the dates or the days of the week in the time range. Then enter the time-range name when applying an ACL to set restrictions to the access list. You can use the time range to define when the permit or deny statements in the ACL are in effect, for example, during a specified time period or on specified days of the week. The **time-range** keyword and argument are referenced in the named and numbered extended ACL task tables.

These are some benefits of using time ranges:

- You have more control over permitting or denying a user access to resources, such as an application (identified by an IP address/mask pair and a port number).
- You can control logging messages. ACL entries can be set to log traffic only at certain times of the day. Therefore, you can simply deny access without needing to analyze many logs generated during peak hours.

Time-based access lists trigger CPU activity because the new configuration of the access list must be merged with other features and the combined configuration loaded into the hardware memory. For this reason, you should be careful not to have several access lists configured to take affect in close succession (within a small number of minutes of each other.)

Note The time range relies on the switch system clock; therefore, you need a reliable clock source. We recommend that you use Network Time Protocol (NTP) to synchronize the switch clock.

Related Topics

Configuring Time Ranges for ACLs, on page 887

IPv4 ACL Interface Considerations

When you apply the **ip access-group** interface configuration command to a Layer 3 interface (an SVI, a Layer 3 EtherChannel, or a routed port), the interface must have been configured with an IP address. Layer 3 access groups filter packets that are routed or are received by Layer 3 processes on the CPU. They do not affect packets bridged within a VLAN.

For inbound ACLs, after receiving a packet, the switch checks the packet against the ACL. If the ACL permits the packet, the switch continues to process the packet. If the ACL rejects the packet, the switch discards the packet.

For outbound ACLs, after receiving and routing a packet to a controlled interface, the switch checks the packet against the ACL. If the ACL permits the packet, the switch sends the packet. If the ACL rejects the packet, the switch discards the packet.

By default, the input interface sends ICMP Unreachable messages whenever a packet is discarded, regardless of whether the packet was discarded because of an ACL on the input interface or because of an ACL on the output interface. ICMP Unreachables are normally limited to no more than one every one-half second per input interface, but this can be changed by using the **ip icmp rate-limit unreachable** global configuration command.

When you apply an undefined ACL to an interface, the switch acts as if the ACL has not been applied to the interface and permits all packets. Remember this behavior if you use undefined ACLs for network security.

Related Topics

Applying an IPv4 ACL to an Interface, on page 890
Restrictions for Configuring IPv4 Access Control Lists, on page 865

How to Configure ACLs

Configuring IPv4 ACLs

These are the steps to use IP ACLs on the switch:

Procedure

Step 1 Create an ACL by specifying an access list number or name and the access conditions.

Step 2 Apply the ACL to interfaces or terminal lines. You can also apply standard and extended IP ACLs to VLAN maps.

Creating a Numbered Standard ACL

Follow these steps to create a numbered standard ACL:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**access-list** *access-list-number* {**deny** | **permit**} *source source-wildcard* [**log**] **Example:** `Switch(config)# access-list 2 deny your_host`	Defines a standard IPv4 access list by using a source address and wildcard. The *access-list-number* is a decimal number from 1 to 99 or 1300 to 1999. Enter **deny** or **permit** to specify whether to deny or permit access if conditions are matched. The *source* is the source address of the network or host from which the packet is being sent specified as: • The 32-bit quantity in dotted-decimal format. • The keyword **any** as an abbreviation for *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard. • The keyword **host** as an abbreviation for source and *source-wildcard* of *source* 0.0.0.0. (Optional) The *source-wildcard* applies wildcard bits to the source. (Optional) Enter **log** to cause an informational logging message about the packet that matches the entry to be sent to the console. **Note** Logging is supported only on ACLs attached to Layer 3 interfaces.

	Command or Action	Purpose
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Configuring VLAN Maps, on page 894

Creating a Numbered Extended ACL

Follow these steps to create a numbered extended ACL:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** tos] [**fragments**] [**log** [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*] **Example:** `Switch(config)# access-list 101 permit ip host 10.1.1.2 any precedence 0 tos 0 log`	Defines an extended IPv4 access list and the access conditions. The *access-list-number* is a decimal number from 100 to 199 or 2000 to 2699. Enter **deny** or **permit** to specify whether to deny or permit the packet if conditions are matched. For *protocol*, enter the name or number of an P protocol: **ahp**, **eigrp**, **esp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **pcp**, **pim**, **tcp**, or **udp**, or an integer in the range 0 to 255

	Command or Action	Purpose
		representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the keyword **ip**. **Note** This step includes options for most IP protocols. For additional specific parameters for TCP, UDP, ICMP, and IGMP, see the following steps. The *source* is the number of the network or host from which the packet is sent. The *source-wildcard* applies wildcard bits to the source. The *destination* is the network or host number to which the packet is sent. The *destination-wildcard* applies wildcard bits to the destination. Source, source-wildcard, destination, and destination-wildcard can be specified as: • The 32-bit quantity in dotted-decimal format. • The keyword **any** for 0.0.0.0 255.255.255.255 (any host). • The keyword **host** for a single host 0.0.0.0. The other keywords are optional and have these meanings: • **precedence**—Enter to match packets with a precedence level specified as a number from 0 to 7 or by name: **routine** (0), **priority** (1), **immediate** (2), **flash** (3), **flash-override** (4), **critical** (5), **internet** (6), **network** (7). • **fragments**—Enter to check non-initial fragments. • **tos**—Enter to match by type of service level, specified by a number from 0 to 15 or a name: **normal** (0), **max-reliability** (2), **max-throughput** (4), **min-delay** (8). • **log**—Enter to create an informational logging message to be sent to the console about the packet that matches the entry or **log-input** to include the input interface in the log entry.

	Command or Action	Purpose
		• **time-range**—Specify the time-range name. • **dscp**—Enter to match packets with the DSCP value specified by a number from 0 to 63, or use the question mark (?) to see a list of available values. **Note** If you enter a **dscp** value, you cannot enter **tos** or **precedence**. You can enter both a **tos** and a **precedence** value with no **dscp**.
Step 3	**access-list** *access-list-number* {**deny** | **permit**} **tcp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log** [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*] [*flag*] **Example:** `Switch(config)# access-list 101 permit tcp any any eq 500`	Defines an extended TCP access list and the access conditions. The parameters are the same as those described for an extended IPv4 ACL, with these exceptions: (Optional) Enter an *operator* and *port* to compare source (if positioned after *source source-wildcard*) or destination (if positioned after *destination destination-wildcard*) port. Possible operators include **eq** (equal), **gt** (greater than), **lt** (less than), **neq** (not equal), and **range** (inclusive range). Operators require a port number (range requires two port numbers separated by a space). Enter the *port* number as a decimal number (from 0 to 65535) or the name of a TCP port. Use only TCP port numbers or names when filtering TCP. The other optional keywords have these meanings: • **established**—Enter to match an established connection. This has the same function as matching on the **ack** or **rst** flag. • *flag*—Enter one of these flags to match by the specified TCP header bits: **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize), or **urg** (urgent).
Step 4	**access-list** *access-list-number* {**deny** | **permit**} **udp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**]	(Optional) Defines an extended UDP access list and the access conditions. The UDP parameters are the same as those described for TCP except that the [operator

	Command or Action	Purpose
	[**log** [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*] **Example:** `Switch(config)# access-list 101 permit udp any any eq 100`	[port]] port number or name must be a UDP port number or name, and the **flag** and **established** keywords are not valid for UDP.
Step 5	**access-list** *access-list-number* {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* | [[*icmp-type icmp-code*] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log** [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*] **Example:** `Switch(config)# access-list 101 permit icmp any any 200`	Defines an extended ICMP access list and the access conditions. The ICMP parameters are the same as those described for most IP protocols in an extended IPv4 ACL, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings: • *icmp-type*—Enter to filter by ICMP message type, a number from 0 to 255. • *icmp-code*—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255. • *icmp-message*—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name.
Step 6	**access-list** *access-list-number* {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log** [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*] **Example:** `Switch(config)# access-list 101 permit igmp any any 14`	(Optional) Defines an extended IGMP access list and the access conditions. The IGMP parameters are the same as those described for most IP protocols in an extended IPv4 ACL, with this optional parameter. *igmp-type*—To match IGMP message type, enter a number from 0 to 15, or enter the message name: **dvmrp**, **host-query**, **host-report**, **pim**, or **trace**.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Related Topics

Configuring VLAN Maps, on page 894

Creating Named Standard ACLs

Follow these steps to create a standard ACL using names:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip access-list standard** *name* **Example:** `Switch(config)# ip access-list standard 20`	Defines a standard IPv4 access list using a name, and enter access-list configuration mode. The name can be a number from 1 to 99.

Step 4	Use one of the following:
	• **deny** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**]
	• **permit** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**]
	Example:
	`Switch(config-std-nacl)# deny 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255`
	or
	`Switch(config-std-nacl)# permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0`
		In access-list configuration mode, specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.
		• **host** *source*—A source and source wildcard of *source* 0.0.0.0.
		• **any**—A source and source wildcard of 0.0.0.0 255.255.255.255.

Step 5	**end** **Example:** `Switch(config-std-nacl)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Creating Extended Named ACLs

Follow these steps to create an extended ACL using names:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip access-list extended** *name* **Example:** `Switch(config)# ip access-list extended 150`	Defines an extended IPv4 access list using a name, and enter access-list configuration mode. The name can be a number from 100 to 199.
Step 4	{**deny** | **permit**} *protocol* {*source* [*source-wildcard*] | **host** *source* | **any**} {*destination* [*destination-wildcard*] | host *destination* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log**] [**time-range** *time-range-name*] **Example:**	In access-list configuration mode, specify the conditions allowed or denied. Use the **log** keyword to get access list logging messages, including violations. • **host** *source*—A source and source wildcard of *source* 0.0.0.0.

	Command or Action	Purpose
	`Switch(config-ext-nacl)# permit 0 any any`	• **host** *destintation*—A destination and destination wildcard of *destination* 0.0.0.0. • **any**—A source and source wildcard or destination and destination wildcard of 0.0.0.0 255.255.255.255.
Step 5	**end** **Example:** `Switch(config-ext-nacl)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

When you are creating extended ACLs, remember that, by default, the end of the ACL contains an implicit deny statement for everything if it did not find a match before reaching the end. For standard ACLs, if you omit the mask from an associated IP host address access list specification, 0.0.0.0 is assumed to be the mask.

After you create an ACL, any additions are placed at the end of the list. You cannot selectively add ACL entries to a specific ACL. However, you can use **no permit** and **no deny** access-list configuration mode commands to remove entries from a named ACL.

Being able to selectively remove lines from a named ACL is one reason you might use named ACLs instead of numbered ACLs.

What to do next

After creating a named ACL, you can apply it to interfaces or to VLANs .

Configuring Time Ranges for ACLs

Follow these steps to configure a time-range parameter for an ACL:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch(config)# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**time-range** *time-range-name* **Example:** `Switch(config)# time-range workhours`	Assigns a meaningful name (for example, *workhours*) to the time range to be created, and enter time-range configuration mode. The name cannot contain a space or quotation mark and must begin with a letter.

Step 4	Use one of the following:
	• **absolute** [**start** *time date*] [**end** *time date*]
	• **periodic** *day-of-the-week hh:mm to* [*day-of-the-week*] *hh:mm*
	• **periodic** {**weekdays** | **weekend** | **daily**} *hh:mm to hh:mm*
	Example:
	`Switch(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006`
	or
	`Switch(config-time-range)# periodic weekdays 8:00 to 12:00`
		Specifies when the function it will be applied to is operational.
		• You can use only one **absolute** statement in the time range. If you configure more than one absolute statement, only the one configured last is executed.
		• You can enter multiple **periodic** statements. For example, you could configure different hours for weekdays and weekends.
		See the example configurations.

Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.

	Command or Action	Purpose
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

Repeat the steps if you have multiple items that you want in effect at different times.

Related Topics

Time Ranges for ACLs, on page 878

Applying an IPv4 ACL to a Terminal Line

You can use numbered ACLs to control access to one or more terminal lines. You cannot apply named ACLs to lines. You must set identical restrictions on all the virtual terminal lines because a user can attempt to connect to any of them.

Follow these steps to restrict incoming and outgoing connections between a virtual terminal line and the addresses in an ACL:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch(config)# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**line** [**console** | **vty**] *line-number* **Example:** `Switch(config)# line console 0`	Identifies a specific line to configure, and enter in-line configuration mode. • **console**—Specifies the console terminal line. The console port is DCE. • **vty**—Specifies a virtual terminal for remote console access. The *line-number* is the first line number in a contiguous group that you want to configure

	Command or Action	Purpose
		when the line type is specified. The range is from 0 to 16.
Step 4	**access-class** *access-list-number* {**in** | **out**} **Example:** `Switch(config-line)# access-class 10 in`	Restricts incoming and outgoing connections between a particular virtual terminal line (into a device) and the addresses in an access list.
Step 5	**end** **Example:** `Switch(config-line)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Applying an IPv4 ACL to an Interface

This section describes how to apply IPv4 ACLs to network interfaces.

Beginning in privileged EXEC mode, follow these steps to control access to an interface:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface`	Identifies a specific interface for configuration, and enter interface configuration mode. The interface can be a Layer 2 interface (port ACL), or a Layer 3 interface (router ACL).

	Command or Action	Purpose
	`gigabitethernet1/0/1`	
Step 3	**ip access-group** {*access-list-number* | *name*} {**in** | **out**} **Example:** `Switch(config-if)# ip access-group 2 in`	Controls access to the specified interface.
Step 4	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Displays the access list configuration.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

IPv4 ACL Interface Considerations, on page 879
Restrictions for Configuring IPv4 Access Control Lists, on page 865

Creating Named MAC Extended ACLs

You can filter non-IPv4 traffic on a VLAN or on a Layer 2 interface by using MAC addresses and named MAC extended ACLs. The procedure is similar to that of configuring other extended named ACLs.

Follow these steps to create a named MAC extended ACL:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**mac access-list extended** *name* **Example:** `Switch(config)# mac access-list extended mac1`	Defines an extended MAC access list using a name.

Step 4	{**deny** | **permit**} {**any** | **host** *source MAC address* | *source MAC address mask*} {**any** | **host** *destination MAC address* | *destination MAC address mask*} [*type mask* | **lsap** *lsap mask* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp** | 0-*65535*] [**cos** *cos*]
	Example:
	`Switch(config-ext-macl)# deny any any decnet-iv`
	or
	`Switch(config-ext-macl)# permit any any`
		In extended MAC access-list configuration mode, specifies to **permit** or **deny** any source MAC address, a source MAC address with a mask, or a specific **host** source MAC address and **any** destination MAC address, destination MAC address with a mask, or a specific destination MAC address.
		(Optional) You can also enter these options:
		• *type mask*—An arbitrary EtherType number of a packet with Ethernet II or SNAP encapsulation in decimal, hexadecimal, or octal with optional mask of *don't care* bits applied to the EtherType before testing for a match.
		• **lsap** *lsap mask*—An LSAP number of a packet with IEEE 802.2 encapsulation in decimal, hexadecimal, or octal with optional mask of *don't care* bits.
		• **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**—A non-IP protocol.
		• **cos** *cos*—An IEEE 802.1Q cost of service number from 0 to 7 used to set priority.

Step 5	**end** **Example:** `Switch(config-ext-macl)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Restrictions for Configuring IPv4 Access Control Lists, on page 865
Configuring VLAN Maps, on page 894

Applying a MAC ACL to a Layer 2 Interface

Follow these steps to apply a MAC access list to control access to a Layer 2 interface:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/2`	Identifies a specific interface, and enter interface configuration mode. The interface must be a physical Layer 2 interface (port ACL).
Step 4	**mac access-group** {*name*} {**in** | **out** } **Example:** `Switch(config-if)# mac access-group mac1`	Controls access to the specified interface by using the MAC access list. Port ACLs are supported in the outbound and inbound directions .

	Command or Action	Purpose
	`in`	
Step 5	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show mac access-group** [**interface** *interface-id*] **Example:** `Switch# show mac access-group interface gigabitethernet1/0/2`	Displays the MAC access list applied to the interface or all Layer 2 interfaces.
Step 7	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 8	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

After receiving a packet, the switch checks it against the inbound ACL. If the ACL permits it, the switch continues to process the packet. If the ACL rejects the packet, the switch discards it. When you apply an undefined ACL to an interface, the switch acts as if the ACL has not been applied and permits all packets. Remember this behavior if you use undefined ACLs for network security.

Related Topics

Restrictions for Configuring IPv4 Access Control Lists, on page 865

Configuring VLAN Maps

To create a VLAN map and apply it to one or more VLANs, perform these steps:

Before you begin

Create the standard or extended IPv4 ACLs or named MAC extended ACLs that you want to apply to the VLAN.

Procedure

	Command or Action	Purpose
Step 1	**vlan access-map** *name* [**number**] **Example:** `Switch(config)# vlan access-map map_1 20`	Creates a VLAN map, and give it a name and (optionally) a number. The number is the sequence number of the entry within the map. When you create VLAN maps with the same name, numbers are assigned sequentially in increments of 10. When modifying or deleting maps, you can enter the number of the map entry that you want to modify or delete. VLAN maps do not use the specific permit or deny keywords. To deny a packet by using VLAN maps, create an ACL that would match the packet, and set the action to drop. A permit in the ACL counts as a match. A deny in the ACL means no match. Entering this command changes to access-map configuration mode.
Step 2	**match** {**ip** | **mac**} **address** {*name* | *number*} [*name* | *number*] **Example:** `Switch(config-access-map)# match ip address ip2`	Match the packet (using either the IP or MAC address) against one or more standard or extended access lists. Note that packets are only matched against access lists of the correct protocol type. IP packets are matched against standard or extended IP access lists. Non-IP packets are only matched against named MAC extended access lists. **Note** If the VLAN map is configured with a match clause for a type of packet (IP or MAC) and the map action is drop, all packets that match the type are dropped. If the VLAN map has no match clause, and the configured action is drop, all IP and Layer 2 packets are dropped.
Step 3	Enter one of the following commands to specify an IP packet or a non-IP packet (with only a known MAC address) and to match the packet against one or more ACLs (standard or extended): • **action** { **forward**} `Switch(config-access-map)# action forward` • **action** { **drop**}	Sets the action for the map entry.

	Command or Action	Purpose
	`Switch(config-access-map)# action drop`	
Step 4	**vlan filter** *mapname* **vlan-list** *list* **Example:** `Switch(config)# vlan filter map 1 vlan-list 20-22`	Applies the VLAN map to one or more VLAN IDs. The list can be a single VLAN ID (22), a consecutive list (10-22), or a string of VLAN IDs (12, 22, 30). Spaces around the comma and hyphen are optional.

Related Topics

Creating a Numbered Standard ACL, on page 880
Creating a Numbered Extended ACL, on page 881
Creating Named MAC Extended ACLs, on page 891
Creating a VLAN Map, on page 896
Applying a VLAN Map to a VLAN, on page 897

Creating a VLAN Map

Each VLAN map consists of an ordered series of entries. Beginning in privileged EXEC mode, follow these steps to create, add to, or delete a VLAN map entry:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**vlan access-map** *name* [**number**] **Example:** `Switch(config)# vlan access-map map_1 20`	Creates a VLAN map, and give it a name and (optionally) a number. The number is the sequence number of the entry within the map. When you create VLAN maps with the same name, numbers are assigned sequentially in increments of 10. When modifying or deleting maps, you can enter the number of the map entry that you want to modify or delete. VLAN maps do not use the specific permit or deny keywords. To deny a packet by using VLAN maps, create an ACL that would match the packet, and set the action to drop. A permit

	Command or Action	Purpose
		in the ACL counts as a match. A deny in the ACL means no match. Entering this command changes to access-map configuration mode.
Step 3	**match** {**ip** | **mac**} **address** {*name* | *number*} [*name* | *number*] **Example:** `Switch(config-access-map)# match ip address ip2`	Match the packet (using either the IP or MAC address) against one or more standard or extended access lists. Note that packets are only matched against access lists of the correct protocol type. IP packets are matched against standard or extended IP access lists. Non-IP packets are only matched against named MAC extended access lists.
Step 4	**action** {**drop** | **forward**} **Example:** `Switch(config-access-map)# action forward`	(Optional) Sets the action for the map entry. The default is to forward.
Step 5	**end** **Example:** `Switch(config-access-map)# end`	Returns to global configuration mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Displays the access list configuration.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Configuring VLAN Maps, on page 894

Applying a VLAN Map to a VLAN

Beginning in privileged EXEC mode, follow these steps to apply a VLAN map to one or more VLANs:

Procedure

	Command or Action	Purpose
Step 1		
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**vlan filter** *mapname* **vlan-list** *list* **Example:** `Switch(config)# vlan filter map 1 vlan-list 20-22`	Applies the VLAN map to one or more VLAN IDs. The list can be a single VLAN ID (22), a consecutive list (10-22), or a string of VLAN IDs (12, 22, 30). Spaces around the comma and hyphen are optional.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Displays the access list configuration.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Configuring VLAN Maps, on page 894

Configuring VACL Logging

Beginning in privileged EXEC mode:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters the global configuration mode.

	Command or Action	Purpose
	`Switch# configure terminal`	
Step 2	**vlan access-map name** [*number*] **Example:** `Switch(config)# vlan access-map gandymede 10`	Creates a VLAN map. Give it a name and optionally a number. The number is the sequence number of the entry within the map. The sequence number range is from 0 to 65535. When you create VLAN maps with the same name, numbers are assigned sequentially in increments of 10. When modifying or deleting maps, you can enter the number of the map entry that you want to modify or delete. Specifying the map name and optionally a number enters the access-map configuration mode.
Step 3	**action drop log** **Example:** `Switch(config-access-map)# action drop log`	Sets the VLAN access map to drop and log IP packets.
Step 4	**exit** **Example:** `Switch(config-access-map)# exit`	Exits the VLAN access map configuration mode and return to the global configuration mode.
Step 5	**vlan access-log** {**maxflow** *max_number* | **threshold** *pkt_count*} **Example:** `Switch(config)# vlan access-log threshold 4000`	Configures the VACL logging parameters. • **maxflow** *max_number*—Sets the log table size. The content of the log table can be deleted by setting the **maxflow** to 0. When the log table is full, the software drops logged packets from new flows. The range is from 0 to 2048. The default is 500. • **threshold** *pkt_count*—Sets the logging threshold. A logging message is generated if the threshold for a flow is reached before the 5-minute interval. The threshold range is from 0 to 2147483647. The default threshold is 0, which means that a syslog message is generated every 5 minutes.

	Command or Action	Purpose
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Monitoring IPv4 ACLs

You can monitor IPv4 ACLs by displaying the ACLs that are configured on the switch, and displaying the ACLs that have been applied to interfaces and VLANs.

When you use the **ip access-group** interface configuration command to apply ACLs to a Layer 2 or 3 interface, you can display the access groups on the interface. You can also display the MAC ACLs applied to a Layer 2 interface. You can use the privileged EXEC commands as described in this table to display this information.

Table 65: Commands for Displaying Access Lists and Access Groups

Command	Purpose
show access-lists [*number* | *name*]	Displays the contents of one or all current IP and MAC address access lists or a specific access list (numbered or named).
show ip access-lists [*number* | *name*]	Displays the contents of all current IP access lists or a specific IP access list (numbered or named).
show ip interface *interface-id*	Displays detailed configuration and status of an interface. If IP is enabled on the interface and ACLs have been applied by using the **ip access-group** interface configuration command, the access groups are included in the display.
show running-config [**interface** *interface-id*]	Displays the contents of the configuration file for the switch or the specified interface, including all configured MAC and IP access lists and which access groups are applied to an interface.
show mac access-group [**interface** *interface-id*]	Displays MAC access lists applied to all Layer 2 interfaces or the specified Layer 2 interface.

Configuration Examples for ACLs

Examples: Using Time Ranges with ACLs

This example shows how to verify after you configure time ranges for *workhours* and to configure January 1, 2006, as a company holiday.

```
Switch# show time-range
time-range entry: new_year_day_2003 (inactive)
   absolute start 00:00 01 January 2006 end 23:59 01 January 2006
time-range entry: workhours (inactive)
   periodic weekdays 8:00 to 12:00
   periodic weekdays 13:00 to 17:00
```

To apply a time range, enter the time-range name in an extended ACL that can implement time ranges. This example shows how to create and verify extended access list 188 that denies TCP traffic from any source to any destination during the defined holiday times and permits all TCP traffic during work hours.

```
Switch(config)# access-list 188 deny tcp any any time-range new_year_day_2006
Switch(config)# access-list 188 permit tcp any any time-range workhours
Switch(config)# end
Switch# show access-lists
Extended IP access list 188
   10 deny tcp any any time-range new_year_day_2006 (inactive)
   20 permit tcp any any time-range workhours (inactive)
```

This example uses named ACLs to permit and deny the same traffic.

```
Switch(config)# ip access-list extended deny_access
Switch(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended may_access
Switch(config-ext-nacl)# permit tcp any any time-range workhours
Switch(config-ext-nacl)# end
Switch# show ip access-lists
Extended IP access list lpip_default
    10 permit ip any any
Extended IP access list deny_access
    10 deny tcp any any time-range new_year_day_2006 (inactive)
Extended IP access list may_access
    10 permit tcp any any time-range workhours (inactive)
```

Examples: Including Comments in ACLs

You can use the **remark** keyword to include comments (remarks) about entries in any IP standard or extended ACL. The remarks make the ACL easier for you to understand and scan. Each remark line is limited to 100 characters.

The remark can go before or after a permit or deny statement. You should be consistent about where you put the remark so that it is clear which remark describes which permit or deny statement. For example, it would

be confusing to have some remarks before the associated permit or deny statements and some remarks after the associated statements.

To include a comment for IP numbered standard or extended ACLs, use the **access-list** *access-list number* **remark** *remark* global configuration command. To remove the remark, use the **no** form of this command.

In this example, the workstation that belongs to Jones is allowed access, and the workstation that belongs to Smith is not allowed access:

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith through
Switch(config)# access-list 1 deny 171.69.3.13
```

For an entry in a named IP ACL, use the **remark** access-list configuration command. To remove the remark, use the **no** form of this command.

In this example, the Jones subnet is not allowed to use outbound Telnet:

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

Examples: Troubleshooting ACLs

If this ACL manager message appears and [chars] is the access-list name,

```
ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

The switch has insufficient resources to create a hardware representation of the ACL. The resources include hardware memory and label space but not CPU memory. A lack of available logical operation units or specialized hardware resources causes this problem. Logical operation units are needed for a TCP flag match or a test other than **eq** (**ne**, **gt**, **lt**, or **range**) on TCP, UDP, or SCTP port numbers.

Use one of these workarounds:

- Modify the ACL configuration to use fewer resources.
- Rename the ACL with a name or number that alphanumerically precedes the ACL names or numbers.

To determine the specialized hardware resources, enter the **show platform layer4 acl** map privileged EXEC command. If the switch does not have available resources, the output shows that index 0 to index 15 are not available.

For more information about configuring ACLs with insufficient resources, see CSCsq63926 in the Bug Toolkit.

For example, if you apply this ACL to an interface:

```
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
permit tcp source source-wildcard destination destination-wildcard
```

And if this message appears:

```
ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

The flag-related operators are not available. To avoid this issue,

- Move the fourth ACE before the first ACE by using **ip access-list resequence** global configuration command:

```
permit tcp source source-wildcard destination destination-wildcard
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
```

  or

- Rename the ACL with a name or number that alphanumerically precedes the other ACLs (for example, rename ACL *79* to ACL *1*).

You can now apply the first ACE in the ACL to the interface. The switch allocates the ACE to available mapping bits in the Opselect index and then allocates flag-related operators to use the same bits in the hardware memory.

IPv4 ACL Configuration Examples

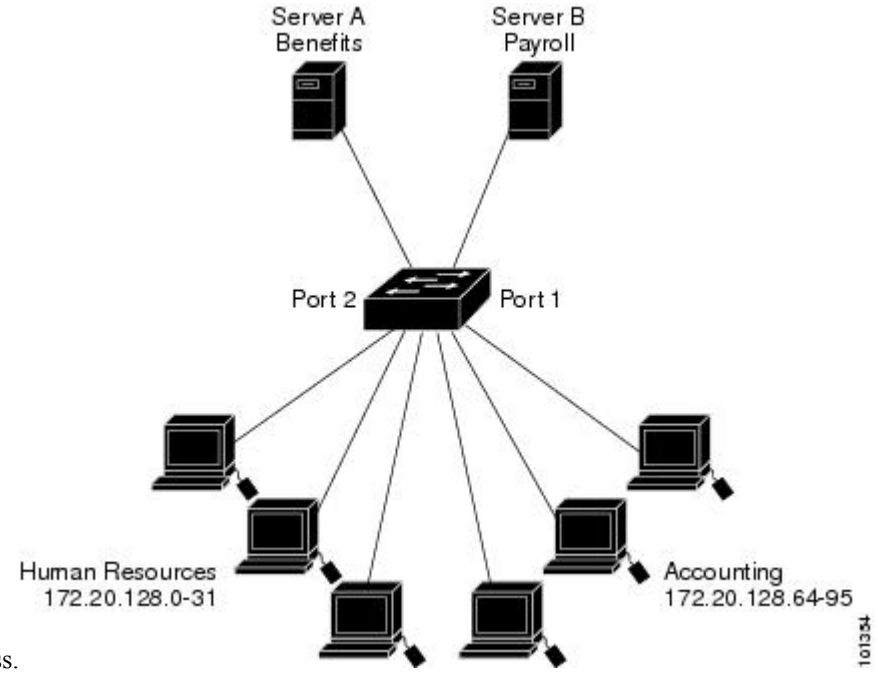
This section provides examples of configuring and applying IPv4 ACLs. For detailed information about compiling ACLs, see the *Cisco IOS Security Configuration Guide, Release 12.4* and to the Configuring IP Services" section in the "IP Addressing and Services" chapter of the *Cisco IOS IP Configuration Guide, Release 12.4*.

ACLs in a Small Networked Office

Figure 46: Using Router ACLs to Control Traffic

This shows a small networked office environment with routed Port 2 connected to Server A, containing benefits and other information that all employees can access, and routed Port 1 connected to Server B, containing

confidential payroll data. All users can access Server A, but Server B has restricted access.



Use router ACLs to do this in one of two ways:

- Create a standard ACL, and filter traffic coming to the server from Port 1.
- Create an extended ACL, and filter traffic coming from the server into Port 1.

Examples: ACLs in a Small Networked Office

This example uses a standard ACL to filter traffic coming into Server B from a port, permitting traffic only from Accounting's source addresses 172.20.128.64 to 172.20.128.95. The ACL is applied to traffic coming out of routed Port 1 from the specified source address.

```
Switch(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Switch(config)# end
Switch# how access-lists
Standard IP access list 6
    10 permit 172.20.128.64, wildcard bits 0.0.0.31
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 6 out
```

This example uses an extended ACL to filter traffic coming from Server B into a port, permitting traffic from any source address (in this case Server B) to only the Accounting destination addresses 172.20.128.64 to 172.20.128.95. The ACL is applied to traffic going into routed Port 1, permitting it to go only to the specified destination addresses. Note that with extended ACLs, you must enter the protocol (IP) before the source and destination information.

```
Switch(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# end
Switch# show access-lists
Extended IP access list 106
```

```
    10 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 106 in
```

Example: Numbered ACLs

In this example, network 36.0.0.0 is a Class A network whose second octet specifies a subnet; that is, its subnet mask is 255.255.0.0. The third and fourth octets of a network 36.0.0.0 address specify a particular host. Using access list 2, the switch accepts one address on subnet 48 and reject all others on that subnet. The last line of the list shows that the switch accepts addresses on all other network 36.0.0.0 subnets. The ACL is applied to packets entering a port.

```
Switch(config)# access-list 2 permit 36.48.0.3
Switch(config)# access-list 2 deny 36.48.0.0 0.0.255.255
Switch(config)# access-list 2 permit 36.0.0.0 0.255.255.255
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ip access-group 2 in
```

Examples: Extended ACLs

In this example, the first line permits any incoming TCP connections with destination ports greater than 1023. The second line permits incoming TCP connections to the Simple Mail Transfer Protocol (SMTP) port of host 128.88.1.2. The third line permits incoming ICMP messages for error feedback.

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# access-list 102 permit icmp any any
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ip access-group 102 in
```

In this example, suppose that you have a network connected to the Internet, and you want any host on the network to be able to form TCP connections to any host on the Internet. However, you do not want IP hosts to be able to form TCP connections to hosts on your network, except to the mail (SMTP) port of a dedicated mail host.

SMTP uses TCP port 25 on one end of the connection and a random port number on the other end. The same port numbers are used throughout the life of the connection. Mail packets coming in from the Internet have a destination port of 25. Outbound packets have the port numbers reversed. Because the secure system of the network always accepts mail connections on port 25, the incoming and outgoing services are separately controlled. The ACL must be configured as an input ACL on the outbound interface and an output ACL on the inbound interface.

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 102 in
```

In this example, the network is a Class B network with the address 128.88.0.0, and the mail host address is 128.88.1.2. The **established** keyword is used only for the TCP to show an established connection. A match occurs if the TCP datagram has the ACK or RST bits set, which show that the packet belongs to an existing connection. Gigabit Ethernet interface 1 on stack member 1 is the interface that connects the router to the Internet.

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 102 in
```

Examples: Named ACLs

Creating named standard and extended ACLs

This example creates a standard ACL named *internet_filter* and an extended ACL named *marketing_group*. The *internet_filter* ACL allows all traffic from the source address 1.2.3.4.

```
Switch(config)# ip access-list standard Internet_filter
Switch(config-ext-nacl)# permit 1.2.3.4
Switch(config-ext-nacl)# exit
```

The *marketing_group* ACL allows any TCP Telnet traffic to the destination address and wildcard 171.69.0.0 0.0.255.255 and denies any other TCP traffic. It permits ICMP traffic, denies UDP traffic from any source to the destination address range 171.69.0.0 through 179.69.255.255 with a destination port less than 1024, denies any other IP traffic, and provides a log of the result.

```
Switch(config)# ip access-list extended marketing_group
Switch(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Switch(config-ext-nacl)# deny tcp any any
Switch(config-ext-nacl)# permit icmp any any
Switch(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
Switch(config-ext-nacl)# deny ip any any log
Switch(config-ext-nacl)# exit
```

The *Internet_filter* ACL is applied to outgoing traffic and the *marketing_group* ACL is applied to incoming traffic on a Layer 3 port.

```
Switch(config)# interface gigabitethernet3/0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 2.0.5.1 255.255.255.0
Switch(config-if)# ip access-group Internet_filter out
Switch(config-if)# ip access-group marketing_group in
```

Deleting individual ACEs from named ACLs

This example shows how you can delete individual ACEs from the named access list *border-list*:

```
Switch(config)# ip access-list extended border-list
Switch(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

Examples: Time Range Applied to an IP ACL

This example denies HTTP traffic on IP on Monday through Friday between the hours of 8:00 a.m. and 6:00 p.m (18:00). The example allows UDP traffic only on Saturday and Sunday from noon to 8:00 p.m. (20:00).

```
Switch(config)# time-range no-http
Switch(config)# periodic weekdays 8:00 to 18:00
!
Switch(config)# time-range udp-yes
Switch(config)# periodic weekend 12:00 to 20:00
!
Switch(config)# ip access-list extended strict
Switch(config-ext-nacl)# deny tcp any any eq www time-range no-http
Switch(config-ext-nacl)# permit udp any any time-range udp-yes
!
Switch(config-ext-nacl)# exit
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ip access-group strict in
```

Examples: Configuring Commented IP ACL Entries

In this example of a numbered ACL, the workstation that belongs to Jones is allowed access, and the workstation that belongs to Smith is not allowed access:

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith workstation through
Switch(config)# access-list 1 deny 171.69.3.13
```

In this example of a numbered ACL, the Winter and Smith workstations are not allowed to browse the web:

```
Switch(config)# access-list 100 remark Do not allow Winter to browse the web
Switch(config)# access-list 100 deny host 171.69.3.85 any eq www
Switch(config)# access-list 100 remark Do not allow Smith to browse the web
Switch(config)# access-list 100 deny host 171.69.3.13 any eq www
```

In this example of a named ACL, the Jones subnet is not allowed access:

```
Switch(config)# ip access-list standard prevention
Switch(config-std-nacl)# remark Do not allow Jones subnet through
Switch(config-std-nacl)# deny 171.69.0.0 0.0.255.255
```

In this example of a named ACL, the Jones subnet is not allowed to use outbound Telnet:

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp 171.69.0.0 0.0.255.255 any eq telnet
```

Examples: ACL Logging

Two variations of logging are supported on router ACLs. The **log** keyword sends an informational logging message to the console about the packet that matches the entry; the **log-input** keyword includes the input interface in the log entry.

In this example, standard named access list *stan1* denies traffic from 10.1.1.0 0.0.0.255, allows traffic from all other sources, and includes the **log** keyword.

```
Switch(config)# ip access-list standard stan1
Switch(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
Switch(config-std-nacl)# permit any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group stan1 in
Switch(config-if)# end
Switch# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level debugging, 37 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 37 messages logged
    File logging: disabled
    Trap logging: level debugging, 39 message lines logged

Log Buffer (4096 bytes):

00:00:48: NTP: authentication delay calculation problems

<output truncated>

00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet
00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
```

This example is a named extended access list *ext1* that permits ICMP packets from any source to 10.1.1.0 0.0.0.255 and denies all UDP packets.

```
Switch(config)# ip access-list extended ext1
Switch(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
Switch(config-ext-nacl)# deny udp any any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip access-group ext1 in
```

This is a an example of a log for an extended ACL:

```
01:24:23:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 1
packet
01:25:14:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 7
packets
01:26:12:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 1 packet
01:31:33:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 8 packets
```

Note that all logging entries for IP ACLs start with %SEC-6-IPACCESSLOG with minor variations in format depending on the kind of ACL and the access entry that has been matched.

This is an example of an output message when the **log-input** keyword is entered:

```
00:04:21:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 (Vlan1 0001.42ef.a400)
 ->
10.1.1.61 (0/0), 1 packet
```

A log message for the same sort of packet using the **log** keyword does not include the input interface information:

```
00:05:47:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 -> 10.1.1.61 (0/0), 1
 packet
```

Configuration Examples for ACLs and VLAN Maps

Example: Creating an ACL and a VLAN Map to Deny a Packet

This example shows how to create an ACL and a VLAN map to deny a packet. In the first map, any packets that match the *ip1* ACL (TCP packets) would be dropped. You first create the *ip1* ACL to permit any TCP packet and no other packets. Because there is a match clause for IP packets in the VLAN map, the default action is to drop any IP packet that does not match any of the match clauses.

```
Switch(config)# ip access-list extended ip1
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 10
Switch(config-access-map)# match ip address ip1
Switch(config-access-map)# action drop
```

Example: Creating an ACL and a VLAN Map to Permit a Packet

This example shows how to create a VLAN map to permit a packet. ACL *ip2* permits UDP packets and any packets that match the *ip2* ACL are forwarded. In this map, any IP packets that did not match any of the previous ACLs (that is, packets that are not TCP packets or UDP packets) would get dropped.

```
Switch(config)# ip access-list extended ip2
Switch(config-ext-nacl)# permit udp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 20
Switch(config-access-map)# match ip address ip2
Switch(config-access-map)# action forward
```

Example: Default Action of Dropping IP Packets and Forwarding MAC Packets

In this example, the VLAN map has a default action of drop for IP packets and a default action of forward for MAC packets. Used with standard ACL 101 and extended named access lists **igmp-match** and **tcp-match**, the map will have the following results:

- Forward all UDP packets
- Drop all IGMP packets
- Forward all TCP packets
- Drop all other IP packets
- Forward all non-IP packets

```
Switch(config)# access-list 101 permit udp any any
Switch(config)# ip access-list extended igmp-match
Switch(config-ext-nacl)# permit igmp any any

Switch(config)# action forward
```

```
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-ip-default 10
Switch(config-access-map)# match ip address 101
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 20
Switch(config-access-map)# match ip address igmp-match
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 30
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
```

Example: Default Action of Dropping MAC Packets and Forwarding IP Packets

In this example, the VLAN map has a default action of drop for MAC packets and a default action of forward for IP packets. Used with MAC extended access lists **good-hosts** and **good-protocols**, the map will have the following results:

- Forward MAC packets from hosts 0000.0c00.0111 and 0000.0c00.0211
- Forward MAC packets with decnet-iv or vines-ip protocols
- Drop all other non-IP packets
- Forward all IP packets

```
Switch(config)# mac access-list extended good-hosts
Switch(config-ext-macl)# permit host 000.0c00.0111 any
Switch(config-ext-macl)# permit host 000.0c00.0211 any
Switch(config-ext-nacl)# exit
Switch(config)# action forward
Switch(config-ext-macl)# mac access-list extended good-protocols
Switch(config-ext-macl)# permit any any vines-ip
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-mac-default 10
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-mac-default 20
Switch(config-access-map)# match mac address good-protocols
Switch(config-access-map)# action forward
```

Example: Default Action of Dropping All Packets

In this example, the VLAN map has a default action of drop for all packets (IP and non-IP). Used with access lists **tcp-match** and **good-hosts** from Examples 2 and 3, the map will have the following results:

- Forward all TCP packets
- Forward MAC packets from hosts 0000.0c00.0111 and 0000.0c00.0211
- Drop all other IP packets
- Drop all other MAC packets

```
Switch(config)# vlan access-map drop-all-default 10
```

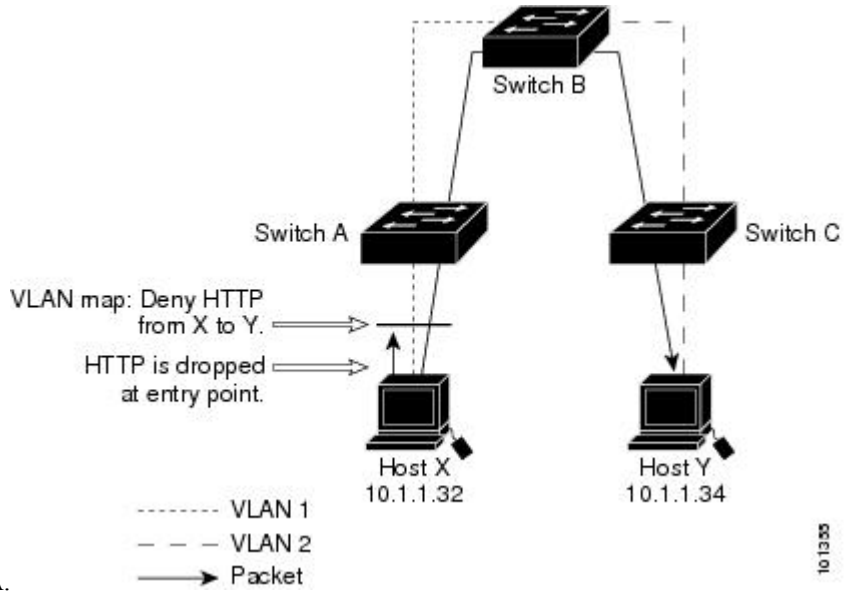
```
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-all-default 20
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
```

Configuration Examples for Using VLAN Maps in Your Network

Example: Wiring Closet Configuration

Figure 47: Wiring Closet Configuration

In a wiring closet configuration, routing might not be enabled on the switch. In this configuration, the switch can still support a VLAN map and a QoS classification ACL. Assume that Host X and Host Y are in different VLANs and are connected to wiring closet switches A and C. Traffic from Host X to Host Y is eventually being routed by Switch B, a Layer 3 switch with routing enabled. Traffic from Host X to Host Y can be access-controlled at the traffic entry point,



Switch A.

If you do not want HTTP traffic switched from Host X to Host Y, you can configure a VLAN map on Switch A to drop all HTTP traffic from Host X (IP address 10.1.1.32) to Host Y (IP address 10.1.1.34) at Switch A and not bridge it to Switch B.

First, define the IP access list *http* that permits (matches) any TCP traffic on the HTTP port.

```
Switch(config)# ip access-list extended http
Switch(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
Switch(config-ext-nacl)# exit
```

Next, create VLAN access map *map2* so that traffic that matches the *http* access list is dropped and all other IP traffic is forwarded.

```
Switch(config)# vlan access-map map2 10
Switch(config-access-map)# match ip address http
```

```
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# ip access-list extended match_all
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map2 20
Switch(config-access-map)# match ip address match_all
Switch(config-access-map)# action forward
```

Then, apply VLAN access map *map2* to VLAN 1.

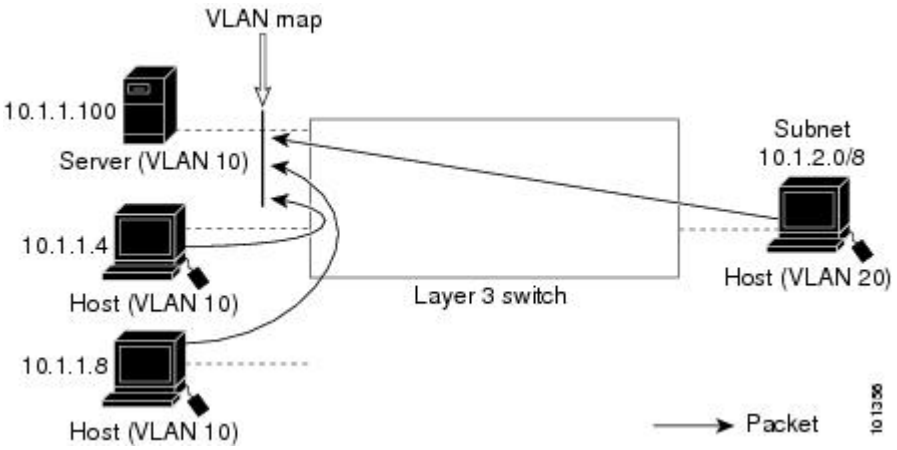
```
Switch(config)# vlan filter map2 vlan 1
```

Example: Restricting Access to a Server on Another VLAN

Figure 48: Restricting Access to a Server on Another VLAN

You can restrict access to a server on another VLAN. For example, server 10.1.1.100 in VLAN 10 needs to have access denied to these hosts:

- Hosts in subnet 10.1.2.0/8 in VLAN 20 should not have access.
- Hosts 10.1.1.4 and 10.1.1.8 in VLAN 10 should not have access.



Example: Denying Access to a Server on Another VLAN

This example shows how to deny access to a server on another VLAN by creating the VLAN map SERVER 1 that denies access to hosts in subnet 10.1.2.0.8, host 10.1.1.4, and host 10.1.1.8 and permits other IP traffic. The final step is to apply the map SERVER1 to VLAN 10.

Define the IP ACL that will match the correct packets.

```
Switch(config)# ip access-list extended SERVER1_ACL
Switch(config-ext-nacl))# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
Switch(config-ext-nacl))# permit ip host 10.1.1.4 host 10.1.1.100
Switch(config-ext-nacl))# permit ip host 10.1.1.8 host 10.1.1.100
Switch(config-ext-nacl))# exit
```

Define a VLAN map using this ACL that will drop IP packets that match SERVER1_ACL and forward IP packets that do not match the ACL.

```
Switch(config)# vlan access-map SERVER1_MAP
Switch(config-access-map)# match ip address SERVER1_ACL
Switch(config-access-map)# action drop
Switch(config)# vlan access-map SERVER1_MAP 20
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
```

Apply the VLAN map to VLAN 10.

```
Switch(config)# vlan filter SERVER1_MAP vlan-list 10
```

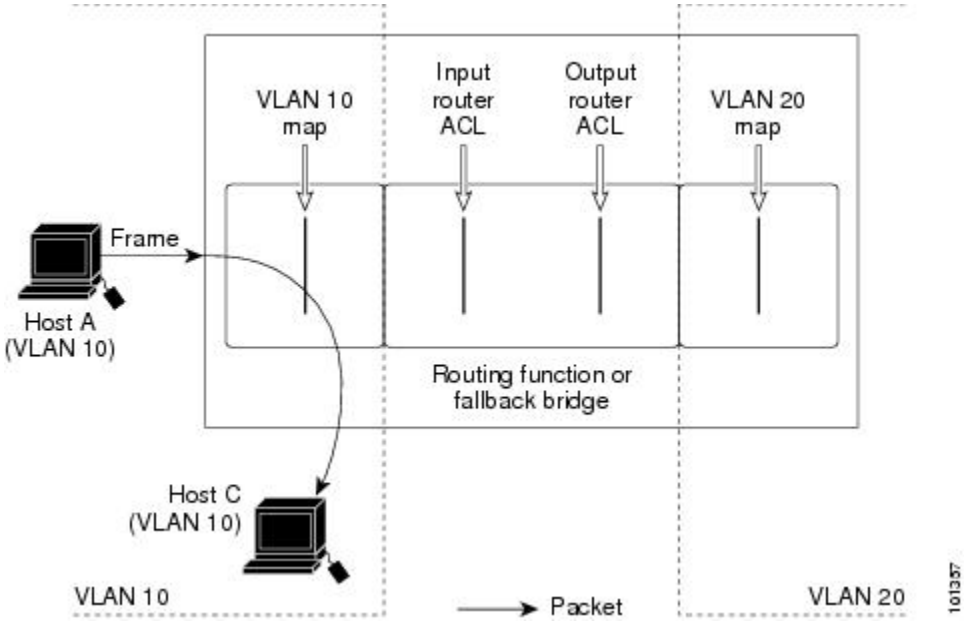
Configuration Examples of Router ACLs and VLAN Maps Applied to VLANs

This section gives examples of applying router ACLs and VLAN maps to a VLAN for switched, bridged, routed, and multicast packets. Although the following illustrations show packets being forwarded to their destination, each time the packet's path crosses a line indicating a VLAN map or an ACL, it is also possible that the packet might be dropped, rather than forwarded.

Example: ACLs and Switched Packets

Figure 49: Applying ACLs on Switched Packets

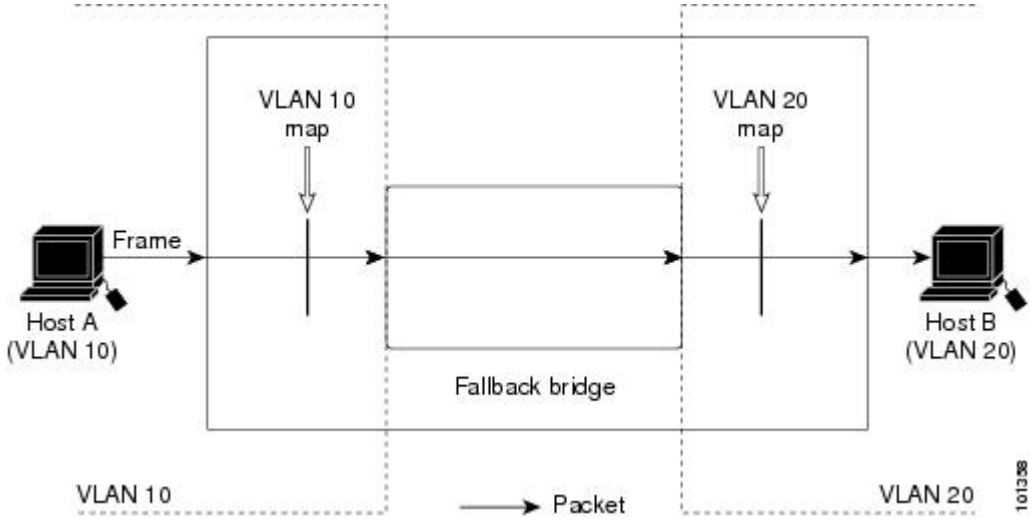
This example shows how an ACL is applied on packets that are switched within a VLAN. Packets switched within the VLAN without being routed or forwarded by fallback bridging are only subject to the VLAN map of the input VLAN.



Example: ACLs and Bridged Packets

Figure 50: Applying ACLs on Bridged Packets

This example shows how an ACL is applied on fallback-bridged packets. For bridged packets, only Layer 2 ACLs are applied to the input VLAN. Only non-IP, non-ARP packets can be fallback-bridged.

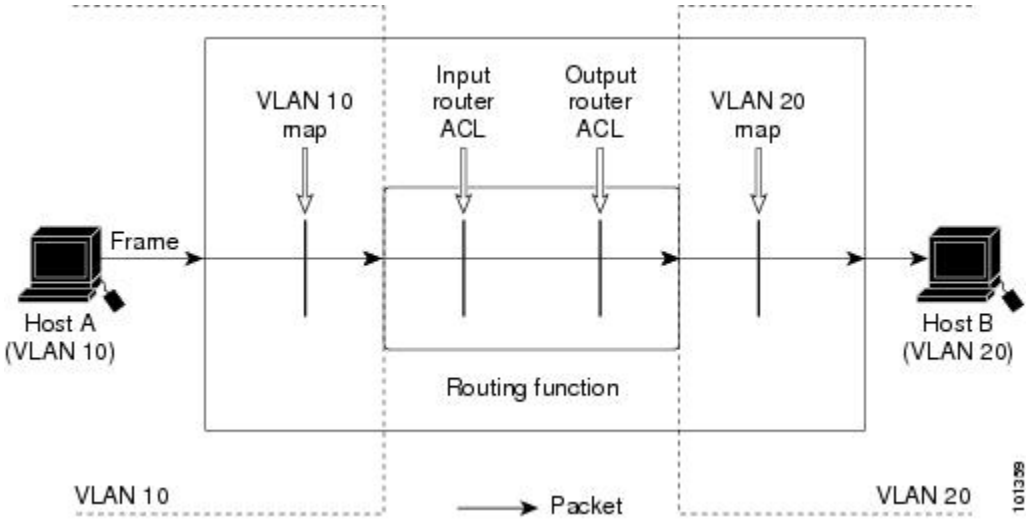


Example: ACLs and Routed Packets

Figure 51: Applying ACLs on Routed Packets

This example shows how ACLs are applied on routed packets. The ACLs are applied in this order:

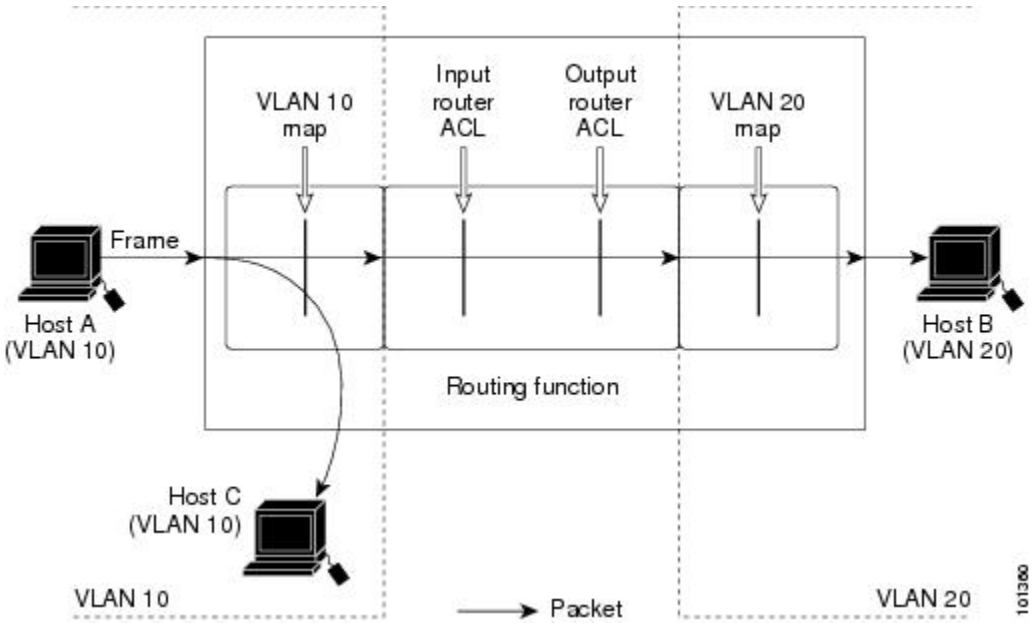
1. VLAN map for input VLAN
2. Input router ACL
3. Output router ACL
4. VLAN map for output VLAN



Example: ACLs and Multicast Packets

Figure 52: Applying ACLs on Multicast Packets

This example shows how ACLs are applied on packets that are replicated for IP multicasting. A multicast packet being routed has two different kinds of filters applied: one for destinations that are other ports in the input VLAN and another for each of the destinations that are in other VLANs to which the packet has been routed. The packet might be routed to more than one output VLAN, in which case a different router output ACL and VLAN map would apply for each destination VLAN. The final result is that the packet might be permitted in some of the output VLANs and not in others. A copy of the packet is forwarded to those destinations where it is permitted. However, if the input VLAN map drops the packet, no destination receives a copy of the packet.



Additional References

Related Documents

Related Topic	Document Title
IPv4 Access Control List topics	Securing the Data Plane Configuration Guide Library, Cisco IOS XE Release 3SE (Cata http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secda

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

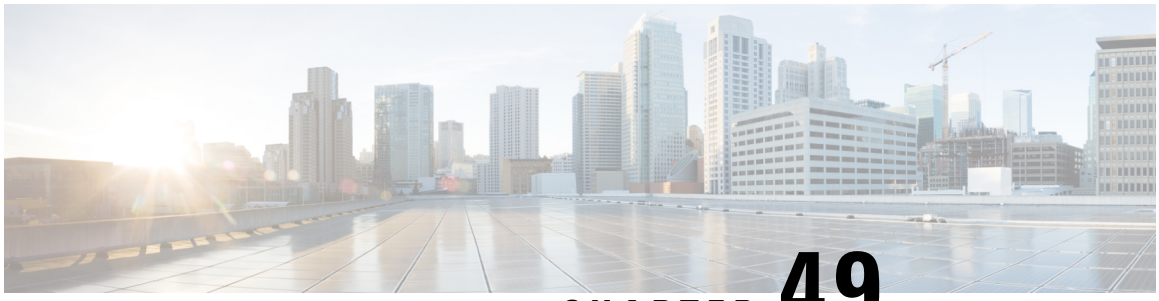
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for IPv4 Access Control Lists

Release	Feature Information
Cisco IOS XE 3.2SE	IPv4 Access Control Lists perform packet filtering to control which packets move through the network and where. Such control provides security by helping to limit network traffic, restrict the access of users and devices to the network, and prevent traffic from leaving a network. This feature was introduced.
Cisco IOS 15.2(2)E	The Named ACL Support for Noncontiguous Ports on an Access Control Entry feature allows you to specify noncontiguous ports in a single access control entry, which greatly reduces the number of entries required in an access control list when several entries have the same source address, destination address, and protocol, but differ only in the ports.
Cisco IOS 15.2(2)E	The IP Access List Entry Sequence Numbering feature helps users to apply sequence numbers to permit or deny statements and also reorder, add, or remove such statements from a named IP access list. This feature makes revising IP access lists much easier. Prior to this feature, users could add access list entries to the end of an access list only; therefore needing to add statements anywhere except the end required reconfiguring the access list entirely. The following commands were introduced or modified: **deny (IP)**, **ip access-list resequence deny (IP)**, **permit (IP)**.



CHAPTER 49

Configuring IPv6 ACLs

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

IPv6 ACLs Overview

You can filter IP Version 6 (IPv6) traffic by creating IPv6 access control lists (ACLs) and applying them to interfaces similar to how you create and apply IP Version 4 (IPv4) named ACLs. You can also create and apply input router ACLs to filter Layer 3 management traffic when the switch is running IP base and LAN base feature sets.

A switch supports three types of IPv6 ACLs:

- IPv6 router ACLs are supported on outbound or inbound traffic on Layer 3 interfaces, which can be routed ports, switch virtual interfaces (SVIs), or Layer 3 EtherChannels. IPv6 router ACLs apply only to IPv6 packets that are routed.
- IPv6 port ACLs are supported on outbound and inbound Layer 2 interfaces. IPv6 port ACLs are applied to all IPv6 packets entering the interface.

- VLAN ACLs or VLAN maps access-control all packets in a VLAN. You can use VLAN maps to filter traffic between devices in the same VLAN. ACL VLAN maps are applied on L2 VLANs. VLAN maps are configured to provide access control based on Layer 3 addresses for IPv6. Unsupported protocols are access-controlled through MAC addresses using Ethernet ACEs. After a VLAN map is applied to a VLAN, all packets entering the VLAN are checked against the VLAN map.

The switch supports VLAN ACLs (VLAN maps) for IPv6 traffic.

You can apply both IPv4 and IPv6 ACLs to an interface. As with IPv4 ACLs, IPv6 port ACLs take precedence over router ACLs.

Switch Stacks and IPv6 ACLs

The active switch supports IPv6 ACLs in hardware and distributes the IPv6 ACLs to the stack members.

If a standby switch takes over as the active switch, it distributes the ACL configuration to all stack members. The member switches sync up the configuration distributed by the new active switch and flush out entries that are not required.

When an ACL is modified, attached to, or detached from an interface, the active switch distributes the change to all stack members.

Interactions with Other Features and Switches

- If an IPv6 router ACL is configured to deny a packet, the packet is not routed. A copy of the packet is sent to the Internet Control Message Protocol (ICMP) queue to generate an ICMP unreachable message for the frame.
- If a bridged frame is to be dropped due to a port ACL, the frame is not bridged.
- You can create both IPv4 and IPv6 ACLs on a switch or switch stack, and you can apply both IPv4 and IPv6 ACLs to the same interface. Each ACL must have a unique name; an error message appears if you try to use a name that is already configured.

  You use different commands to create IPv4 and IPv6 ACLs and to attach IPv4 or IPv6 ACLs to the same Layer 2 or Layer 3 interface. If you use the wrong command to attach an ACL (for example, an IPv4 command to attach an IPv6 ACL), you receive an error message.
- You cannot use MAC ACLs to filter IPv6 frames. MAC ACLs can only filter non-IP frames.
- If the hardware memory is full, packets are dropped on the interface and an unload error message is logged.

Restrictions for IPv6 ACLs

With IPv4, you can configure standard and extended numbered IP ACLs, named IP ACLs, and MAC ACLs. IPv6 supports only named ACLs.

The switch supports most Cisco IOS-supported IPv6 ACLs with some exceptions:

- The switch does not support matching on these keywords: **routing header**, and **undetermined-transport**.
- The switch does not support reflexive ACLs (the **reflect** keyword).

- This release supports port ACLs, router ACLs and VLAN ACLs (VLAN maps) for IPv6.
- The switch does not apply MAC-based ACLs on IPv6 frames.
- When configuring an ACL, there is no restriction on keywords entered in the ACL, regardless of whether or not they are supported on the platform. When you apply the ACL to an interface that requires hardware forwarding (physical ports or SVIs), the switch checks to determine whether or not the ACL can be supported on the interface. If not, attaching the ACL is rejected.
- If an ACL is applied to an interface and you attempt to add an access control entry (ACE) with an unsupported keyword, the switch does not allow the ACE to be added to the ACL that is currently attached to the interface.

IPv6 ACLs on the switch have these characteristics:

- Fragmented frames (the **fragments** keyword as in IPv4) are supported
- The same statistics supported in IPv4 are supported for IPv6 ACLs.
- If the switch runs out of hardware space, the packets associated with the ACL are dropped on the interface.
- Logging is supported for router ACLs, but not for port ACLs.
- The switch supports IPv6 address-matching for a full range of prefix-lengths.

Default Configuration for IPv6 ACLs

The default IPv6 ACL configuration is as follows:

```
Switch# show access-lists preauth_ipv6_acl
IPv6 access list preauth_ipv6_acl (per-user)
permit udp any any eq domain sequence 10
permit tcp any any eq domain sequence 20
permit icmp any any nd-ns sequence 30
permit icmp any any nd-na sequence 40
permit icmp any any router-solicitation sequence 50
permit icmp any any router-advertisement sequence 60
permit icmp any any redirect sequence 70
permit udp any eq 547 any eq 546 sequence 80
permit udp any eq 546 any eq 547 sequence 90
deny ipv6 any any sequence 100
```

Configuring IPv6 ACLs

To filter IPv6 traffic, you perform these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Switch> enable`	
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	[**no**]{**ipv6 access-list** *list-name*| **client permit-control-packets**| **log-update threshold**| **role-based** *list-name*} **Example:** `Switch(config)# ipv6 access-list example_acl_list`	Defines an IPv6 ACL name, and enters IPv6 access list configuration mode.
Step 4	[**no**]{**deny** | **permit**} protocol {*source-ipv6-prefix/|prefix-length*|**any threshold**| **host** *source-ipv6-address*} [operator [*port-number*]] { *destination-ipv6-prefix/ prefix-length* | **any** | **host** *destination-ipv6-address*} [operator [*port-number*]][**dscp** *value*] [**fragments**] [**log**] [**log-input**][**sequence** *value*] [**time-range** *name*]	Enter deny or permit to specify whether to deny or permit the packet if conditions are matched. These are the conditions: • For protocol, enter the name or number of an Internet protocol: **ahp**, **esp**, **icmp**, **ipv6**, **pcp**, **stcp**, **tcp**, or **udp**, or an integer in the range 0 to 255 representing an IPv6 protocol number. • The *source-ipv6-prefix/prefix-length* or *destination-ipv6-prefix/ prefix-length* is the source or destination IPv6 network or class of networks for which to set deny or permit conditions, specified in hexadecimal and using 16-bit values between colons (see RFC 2373). • Enter any as an abbreviation for the IPv6 prefix ::/0. • For **host** *source-ipv6-address* or *destination-ipv6-address*, enter the source or destination IPv6 host address for which to set deny or permit conditions, specified in hexadecimal using 16-bit values between colons. • (Optional) For operator, specify an operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range.**

	Command or Action	Purpose
		If the operator follows the *source-ipv6-prefix/prefix-length* argument, it must match the source port. If the operator follows the *destination-ipv6- prefix/prefix-length* argument, it must match the destination port. • (Optional) The **port-number** is a decimal number from 0 to 65535 or the name of a TCP or UDP port. You can use TCP port names only when filtering TCP. You can use UDP port names only when filtering UDP. • (Optional) Enter **dscp** value to match a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63. • (Optional) Enter **fragments** to check noninitial fragments. This keyword is visible only if the protocol is ipv6. • (Optional) Enter **log** to cause an logging message to be sent to the console about the packet that matches the entry. Enter **log-input** to include the input interface in the log entry. Logging is supported only for router ACLs. • (Optional) Enter **routing** to specify that IPv6 packets be routed. • (Optional) Enter **sequence** *value* to specify the sequence number for the access list statement. The acceptable range is from 1 to 4,294,967,295. • (Optional) Enter **time-range** name to specify the time range that applies to the deny or permit statement.
Step 5	{**deny** | **permit**} **tcp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [**operator** [**port-number**]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [operator [*port-number*]] [**ack**] [**dscp** *value*]	(Optional) Define a TCP access list and the access conditions. Enter **tcp** for Transmission Control Protocol. The parameters are the same as those described in Step 3a, with these additional optional parameters:

	Command or Action	Purpose
	[**established**] [**fin**] [**log**] [**log-input**] [**neq** {**port** | protocol}] [**psh**] [**range** {**port** | protocol}] [**rst**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]	• **ack**—Acknowledgment bit set. • **established**—An established connection. A match occurs if the TCP datagram has the ACK or RST bits set. • **fin**—Finished bit set; no more data from sender. • **neq** {*port* | protocol}—Matches only packets that are not on a given port number. • **psh**—Push function bit set. • **range** {*port* | protocol}—Matches only packets in the port number range. • **rst**—Reset bit set. • **syn**—Synchronize bit set. • **urg**—Urgent pointer bit set.
Step 6	{**deny** | **permit**} **udp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [operator [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [operator [*port-number*]] [**dscp** *value*] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**sequence** *value*] [**time-range** *name*]]	(Optional) Define a UDP access list and the access conditions. Enter **udp** for the User Datagram Protocol. The UDP parameters are the same as those described for TCP, except that the [operator [*port*]] port number or name must be a UDP port number or name, and the established parameter is not valid for UDP.
Step 7	{**deny** | **permit**} **icmp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [operator [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [operator [*port-number*]] [*icmp-type* [*icmp-code*] | icmp-message] [**dscp** *value*] [**log**] [**log-input**] [**sequence** *value*] [**time-range** *name*]	(Optional) Define an ICMP access list and the access conditions. Enter **icmp** for Internet Control Message Protocol. The ICMP parameters are the same as those described for most IP protocols in Step 1, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings: • *icmp-type*—Enter to filter by ICMP message type, a number from 0 to 255. • *icmp-code*—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255. • *icmp-message*—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code

	Command or Action	Purpose
		name. To see a list of ICMP message type names and code names, use the ? key or see command reference for this release.
Step 8	**end**	Return to privileged EXEC mode.
Step 9	**show ipv6 access-list**	Verify the access list configuration.
Step 10	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 11	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

Attach the IPv6 ACL to an Interface

Attaching an IPv6 ACL to an Interface

You can apply an ACL to outbound or inbound traffic on Layer 3 interfaces, or to inbound traffic on Layer 2 interfaces. You can also apply ACLs only to inbound management traffic on Layer 3 interfaces.

Follow these steps to control access to an interface:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *interface-id*	Identify a Layer 2 interface (for port ACLs) or Layer 3 interface (for router ACLs) on which to apply an access list, and enter interface configuration mode.
Step 4	**no switchport**	If applying a router ACL, this changes the interface from Layer 2 mode (the default) to Layer 3 mode.
Step 5	**ipv6 address** *ipv6-address*	Configure an IPv6 address on a Layer 3 interface (for router ACLs).
Step 6	**ipv6 traffic-filter** *access-list-name* {**in** | **out**}	Apply the access list to incoming or outgoing traffic on the interface.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 8	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 9	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Monitoring IPv6 ACLs

You can display information about all configured access lists, all IPv6 access lists, or a specific access list by using one or more of the privileged EXEC commands shown in the table below:

Command	Purpose
show access-lists	Displays all access lists configured on the switch.
show ipv6 access-list [*access-list-name*]	Displays all configured IPv6 access lists or the access list specified by name.
show vlan access-map[*map-name*]	Displays VLAN access map configuration.
show vlan filter[**access-map***access-map*| **vlan***vlan-id*]	Displays the mapping between VACLs and VLANs.

This is an example of the output from the show access-lists privileged EXEC command. The output shows all access lists that are configured on the switch or switch stack.

```
Switch # show access-lists
Extended IP access list hello
    10 permit ip any any
IPv6 access list ipv6
    permit ipv6 any any sequence 10
```

This is an example of the output from the **show ipv6 access-list** privileged EXEC command. The output shows only IPv6 access lists configured on the switch or switch stack

```
Switch# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp (8 matches) sequence 10
    permit tcp any any eq telnet (15 matches) sequence 20
    permit udp any any sequence 30
IPv6 access list outbound
    deny udp any any sequence 10
    deny tcp any any eq telnet sequence 20
```

This is an example of the output from the show vlan access-map privileged EXEC command. The output shows VLAN access map information.

```
Switch# show vlan access-map
Vlan access-map "m1"  10
  Match clauses:
    ipv6 address: ip2
  Action: drop
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 security configuration topics	IPv6 Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/config_library/xe-3se/3850/ipv6-xe-3se-3850-librar
IPv6 command reference	IPv6 Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/command/ipv6-xe-3se-3850-cr-book.html

Error Message Decoder

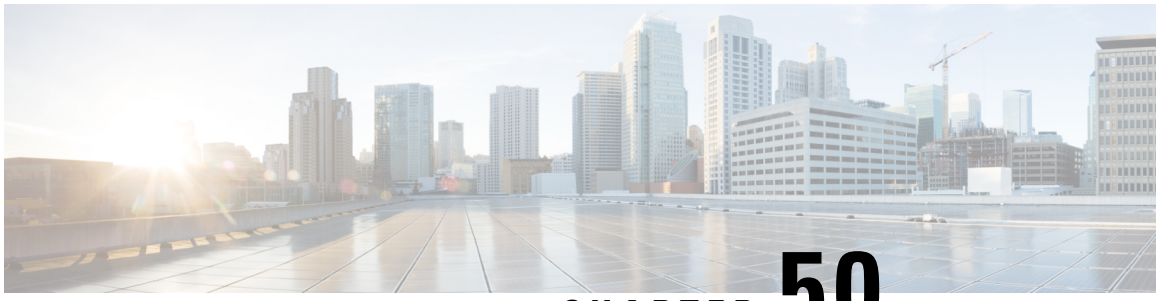
Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support



CHAPTER 50

Configuring DHCP

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About DHCP

DHCP Server

The DHCP server assigns IP addresses from specified address pools on a switch or router to DHCP clients and manages them. If the DHCP server cannot give the DHCP client the requested configuration parameters from its database, it forwards the request to one or more secondary DHCP servers defined by the network administrator. The switch can act as a DHCP server.

DHCP Relay Agent

A DHCP relay agent is a Layer 3 device that forwards DHCP packets between clients and servers. Relay agents forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is different from the normal Layer 2 forwarding, in which IP datagrams are switched transparently between networks. Relay agents receive DHCP messages and generate new DHCP messages to send on output interfaces.

DHCP Snooping

DHCP snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, also referred to as a DHCP snooping binding table.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You use DHCP snooping to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

Note For DHCP snooping to function properly, all DHCP servers must be connected to the switch through trusted interfaces.

An untrusted DHCP message is a message that is received through an untrusted interface. By default, the switch considers all interfaces untrusted. So, the switch must be configured to trust some interfaces to use DHCP Snooping. When you use DHCP snooping in a service-provider environment, an untrusted message is sent from a device that is not in the service-provider network, such as a customer's switch. Messages from unknown devices are untrusted because they can be sources of traffic attacks.

The DHCP snooping binding database has the MAC address, the IP address, the lease time, the binding type, the VLAN number, and the interface information that corresponds to the local untrusted interfaces of a switch. It does not have information regarding hosts interconnected with a trusted interface.

In a service-provider network, an example of an interface you might configure as trusted is one connected to a port on a device in the same network. An example of an untrusted interface is one that is connected to an untrusted interface in the network or to an interface on a device that is not in the network.

When a switch receives a packet on an untrusted interface and the interface belongs to a VLAN in which DHCP snooping is enabled, the switch compares the source MAC address and the DHCP client hardware address. If the addresses match (the default), the switch forwards the packet. If the addresses do not match, the switch drops the packet.

The switch drops a DHCP packet when one of these situations occurs:

- A packet from a DHCP server, such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet, is received from outside the network or firewall.
- A packet is received on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match.
- The switch receives a DHCPRELEASE or DHCPDECLINE broadcast message that has a MAC address in the DHCP snooping binding database, but the interface information in the binding database does not match the interface on which the message was received.
- A DHCP relay agent forwards a DHCP packet that includes a relay-agent IP address that is not 0.0.0.0, or the relay agent forwards a packet that includes option-82 information to an untrusted port.
- The maximum snooping queue size of 1000 is exceeded when DHCP snooping is enabled.

Note This is applicable from Cisco IOS XE Denali 16.1.x release onwards.

If the switch is an aggregation switch supporting DHCP snooping and is connected to an edge switch that is inserting DHCP option-82 information, the switch drops packets with option-82 information when packets are received on an untrusted interface. If DHCP snooping is enabled and packets are received on a trusted port, the aggregation switch does not learn the DHCP snooping bindings for connected devices and cannot build a complete DHCP snooping binding database.

When an aggregation switch can be connected to an edge switch through an untrusted interface and you enter the **ip dhcp snooping information option allow-untrusted** global configuration command, the aggregation switch accepts packets with option-82 information from the edge switch. The aggregation switch learns the bindings for hosts connected through an untrusted switch interface. The DHCP security features, such as dynamic ARP inspection or IP source guard, can still be enabled on the aggregation switch while the switch receives packets with option-82 information on untrusted input interfaces to which hosts are connected. The port on the edge switch that connects to the aggregation switch must be configured as a trusted interface.

Normally, it is not desirable to broadcast packets to wireless clients. So, DHCP snooping replaces destination broadcast MAC address (ffff.ffff.ffff) with unicast MAC address for DHCP packets that are going from server to wireless clients. The unicast MAC address is retrieved from CHADDR field in the DHCP payload. This processing is applied for server to client packets such as DHCP OFFER, DHCP ACK, and DHCP NACK messages. The **ip dhcp snooping wireless bootp-broadcast enable** can be used to revert this behavior. When the wireless BOOTP broadcast is enabled, the broadcast DHCP packets from server are forwarded to wireless clients without changing the destination MAC address.

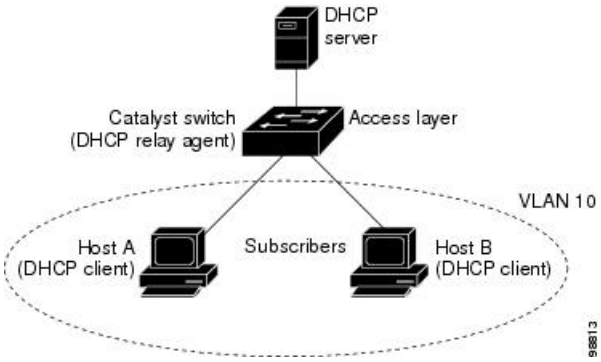
Option-82 Data Insertion

In residential, metropolitan Ethernet-access environments, DHCP can centrally manage the IP address assignments for a large number of subscribers. When the DHCP option-82 feature is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

Note The DHCP option-82 feature is supported only when DHCP snooping is globally enabled on the VLANs to which subscriber devices using option-82 are assigned.

The following illustration shows a metropolitan Ethernet network in which a centralized DHCP server assigns IP addresses to subscribers connected to the switch at the access layer. Because the DHCP clients and their associated DHCP server do not reside on the same IP network or subnet, a DHCP relay agent (the Catalyst switch) is configured with a helper address to enable broadcast forwarding and to transfer DHCP messages between the clients and the server.

Figure 53: DHCP Relay Agent in a Metropolitan Ethernet Network



When you enable the DHCP snooping information option 82 on the switch, the following sequence of events occurs:

- The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- When the switch receives the DHCP request, it adds the option-82 information in the packet. By default, the remote-ID suboption is the switch MAC address, and the circuit-ID suboption is the port identifier, **vlan-mod-port**, from which the packet is received.You can configure the remote ID and circuit ID.
- If the IP address of the relay agent is configured, the switch adds this IP address in the DHCP packet.
- The switch forwards the DHCP request that includes the option-82 field to the DHCP server.
- The DHCP server receives the packet. If the server is option-82-capable, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option-82 field in the DHCP reply.
- The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. The switch verifies that it originally inserted the option-82 data by inspecting the remote ID and possibly the circuit ID fields. The switch removes the option-82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.

In the default suboption configuration, when the described sequence of events occurs, the values in these fields do not change (see the illustration,*Suboption Packet Formats*):

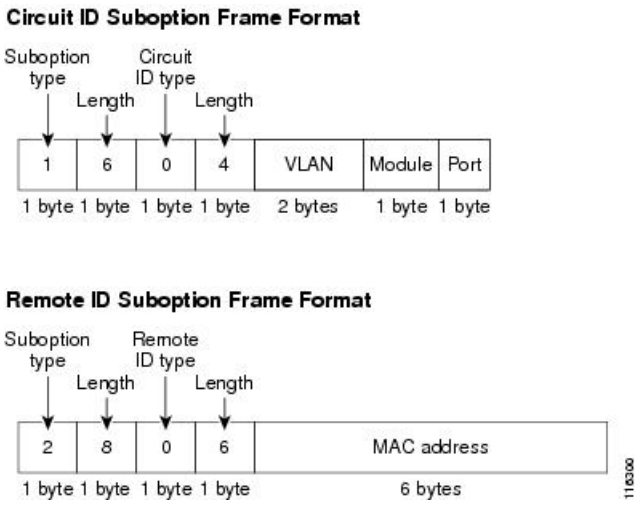
- Circuit-ID suboption fields
  - Suboption type
  - Length of the suboption type
  - Circuit-ID type
  - Length of the circuit-ID type
- Remote-ID suboption fields
  - Suboption type
  - Length of the suboption type
  - Remote-ID type

- Length of the remote-ID type

In the port field of the circuit ID suboption, the port numbers start at 3. For example, on a switch with 24 10/100/1000 ports and four small form-factor pluggable (SFP) module slots, port 3 is the Gigabit Ethernet 1/0/1 port, port 4 is the Gigabit Ethernet 1/0/2 port, and so forth. Port 27 is the SFP module slot Gigabit Ethernet1/0/25, and so forth.

The illustration, *Suboption Packet Formats*. shows the packet formats for the remote-ID suboption and the circuit-ID suboption when the default suboption configuration is used. For the circuit-ID suboption, the module number corresponds to the switch number in the stack. The switch uses the packet formats when you globally enable DHCP snooping and enter the ip dhcp snooping information option global configuration command.

Figure 54: Suboption Packet Formats

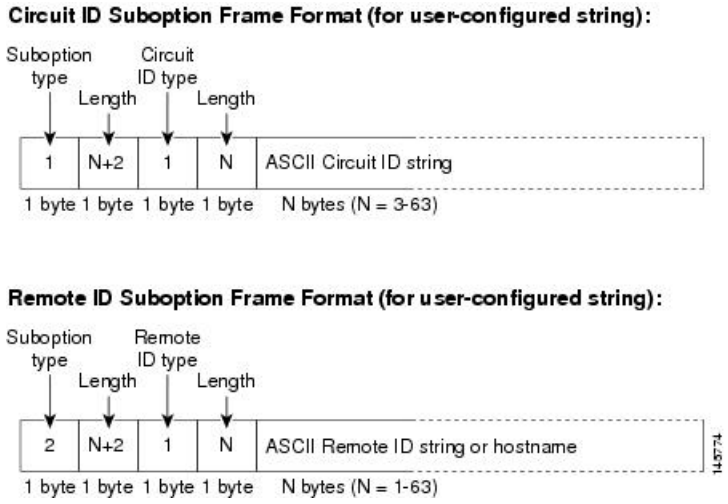


The illustration, *User-Configured Suboption Packet Formats,* shows the packet formats for user-configured remote-ID and circuit-ID suboptions The switch uses these packet formats when DHCP snooping is globally enabled and when the **ip dhcp snooping information option format remote-id** global configuration command and the**ip dhcp snooping vlan information option format-type circuit-id string** interface configuration command are entered.

The values for these fields in the packets change from the default values when you configure the remote-ID and circuit-ID suboptions:

- Circuit-ID suboption fields
  - The circuit-ID type is 1.
  - The length values are variable, depending on the length of the string that you configure.
- Remote-ID suboption fields
  - The remote-ID type is 1.
  - The length values are variable, depending on the length of the string that you configure.

Figure 55: User-Configured Suboption Packet Formats



Cisco IOS DHCP Server Database

During the DHCP-based autoconfiguration process, the designated DHCP server uses the Cisco IOS DHCP server database. It has IP addresses, address bindings, and configuration parameters, such as the boot file.

An address binding is a mapping between an IP address and a MAC address of a host in the Cisco IOS DHCP server database. You can manually assign the client IP address, or the DHCP server can allocate an IP address from a DHCP address pool. For more information about manual and automatic address bindings, see the "Configuring DHCP" chapter of the *Cisco IOS IP Configuration Guide, Release 12.4*.

For procedures to enable and configure the Cisco IOS DHCP server database, see the "DHCP Configuration Task List" section in the "Configuring DHCP" chapter of the *Cisco IOS IP Configuration Guide, Release 12.4*.

DHCP Snooping Binding Database

When DHCP snooping is enabled, the switch uses the DHCP snooping binding database to store information about untrusted interfaces. The database can have up to 64,000 bindings.

Each database entry (binding) has an IP address, an associated MAC address, the lease time (in hexadecimal format), the interface to which the binding applies, and the VLAN to which the interface belongs. The database agent stores the bindings in a file at a configured location. At the end of each entry is a checksum that accounts for all the bytes from the start of the file through all the bytes associated with the entry. Each entry is 72 bytes, followed by a space and then the checksum value.

To keep the bindings when the switch reloads, you must use the DHCP snooping database agent. If the agent is disabled, dynamic ARP inspection or IP source guard is enabled, and the DHCP snooping binding database has dynamic bindings, the switch loses its connectivity. If the agent is disabled and only DHCP snooping is enabled, the switch does not lose its connectivity, but DHCP snooping might not prevent DHCP spoofing attacks.

When reloading, the switch reads the binding file to build the DHCP snooping binding database. The switch updates the file when the database changes.

When a switch learns of new bindings or when it loses bindings, the switch immediately updates the entries in the database. The switch also updates the entries in the binding file. The frequency at which the file is

updated is based on a configurable delay, and the updates are batched. If the file is not updated in a specified time (set by the write-delay and abort-timeout values), the update stops.

This is the format of the file with bindings:

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-..-n>
END
```

Each entry in the file is tagged with a checksum value that the switch uses to verify the entries when it reads the file. The initial-checksum entry on the first line distinguishes entries associated with the latest file update from entries associated with a previous file update.

This is an example of a binding file:

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E Gi1/0/4 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB Gi1/0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB Gi1/0/4 584a38f0
END
```

When the switch starts and the calculated checksum value equals the stored checksum value, the switch reads entries from the binding file and adds the bindings to its DHCP snooping binding database. The switch ignores an entry when one of these situations occurs:

- The switch reads the entry and the calculated checksum value does not equal the stored checksum value. The entry and the ones following it are ignored.
- An entry has an expired lease time (the switch might not remove a binding entry when the lease time expires).
- The interface in the entry no longer exists on the system.
- The interface is a routed interface or a DHCP snooping-trusted interface.

DHCP Snooping and Switch Stacks

DHCP snooping is managed on the stack master. When a new switch joins the stack, the switch receives the DHCP snooping configuration from the stack master. When a member leaves the stack, all DHCP snooping address bindings associated with the switch age out.

All snooping statistics are generated on the stack master. If a new stack master is elected, the statistics counters reset.

When a stack merge occurs, all DHCP snooping bindings in the stack master are lost if it is no longer the stack master. With a stack partition, the existing stack master is unchanged, and the bindings belonging to the

partitioned switches age out. The new master of the partitioned stack begins processing the new incoming DHCP packets.

How to Configure DHCP Features

Default DHCP Snooping Configuration

Table 66: Default DHCP Configuration

Feature	Default Setting
DHCP server	Enabled in Cisco IOS software, requires configuration[11]
DHCP relay agent	Enabled[12]
DHCP packet forwarding address	None configured
Checking the relay agent information	Enabled (invalid messages are dropped)
DHCP relay agent forwarding policy	Replace the existing relay agent information
DHCP snooping enabled globally	Disabled
DHCP snooping information option	Enabled
DHCP snooping option to accept packets on untrusted input interfaces[13]	Disabled
DHCP snooping limit rate	None configured
DHCP snooping trust	Untrusted
DHCP snooping VLAN	Disabled
DHCP snooping MAC address verification	Enabled
Cisco IOS DHCP server binding database	Enabled in Cisco IOS software, requires configuration. **Note** The switch gets network addresses and configuration parameters only from a device configured as a DHCP server.
DHCP snooping binding database agent	Enabled in Cisco IOS software, requires configuration. This feature is operational only when a destination is configured.

11 The switch responds to DHCP requests only if it is configured as a DHCP server.
12 The switch relays DHCP packets only if the IP address of the DHCP server is configured on the SVI of the DHCP client.

[13] Use this feature when the switch is an aggregation switch that receives packets with option-82 information from an edge switch.

DHCP Snooping Configuration Guidelines

- If a switch port is connected to a DHCP server, configure a port as trusted by entering the **ip dhcp snooping trust interface** configuration command.
- If a switch port is connected to a DHCP client, configure a port as untrusted by entering the **no ip dhcp snooping trust** interface configuration command.
- You can display DHCP snooping statistics by entering the **show ip dhcp snooping statistics** user EXEC command, and you can clear the snooping statistics counters by entering the **clear ip dhcp snooping statistics** privileged EXEC command.

Configuring the DHCP Server

The switch can act as a DHCP server.

For procedures to configure the switch as a DHCP server, see the "Configuring DHCP" section of the "IP addressing and Services" section of the *Cisco IOS IP Configuration Guide, Release 12.4*.

DHCP Server and Switch Stacks

The DHCP binding database is managed on the stack master. When a new stack master is assigned, the new master downloads the saved binding database from the TFTP server. When a switchover happens, the new active stack master will use its database file that has been synced from the old active stack master using the SSO function. The IP addresses associated with the lost bindings are released. You should configure an automatic backup by using the **ip dhcp database** *url* [**timeout** *seconds* | **write-delay** *seconds*] global configuration command.

Configuring the DHCP Relay Agent

Follow these steps to enable the DHCP relay agent on the switch:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose
Step 3	**service dhcp** **Example:** `Switch(config)# service dhcp`	Enables the DHCP server and relay agent on your switch. By default, this feature is enabled.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

See the "*Configuring DHCP*" section of the "IP Addressing and Services" section of the *Cisco IOS IP Configuration Guide, Release 12.4* for these procedures:

- Checking (validating) the relay agent information
- Configuring the relay agent forwarding policy

Specifying the Packet Forwarding Address

If the DHCP server and the DHCP clients are on different networks or subnets, you must configure the switch with the **ip helper-address** *address* interface configuration command. The general rule is to configure the command on the Layer 3 interface closest to the client. The address used in the **ip helper-address** command can be a specific DHCP server IP address, or it can be the network address if other DHCP servers are on the destination network segment. Using the network address enables any DHCP server to respond to requests.

Beginning in privileged EXEC mode, follow these steps to specify the packet forwarding address:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Switch> enable`	
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface vlan** *vlan-id* **Example:** `Switch(config)# interface vlan 1`	Creates a switch virtual interface by entering a VLAN ID, and enter interface configuration mode.
Step 4	**ip address** *ip-address subnet-mask* **Example:** `Switch(config-if)# ip address 192.108.1.27 255.255.255.0`	Configures the interface with an IP address and an IP subnet.
Step 5	**ip helper-address** *address* **Example:** `Switch(config-if)# ip helper-address 172.16.1.2`	Specifies the DHCP packet forwarding address. The helper address can be a specific DHCP server address, or it can be the network address if other DHCP servers are on the destination network segment. Using the network address enables other servers to respond to DHCP requests. If you have multiple servers, you can configure one helper address for each server.
Step 6	**end** **Example:** `Switch(config-if)# end`	Returns to global configuration mode.
Step 7	Use one of the following: • **interface range** *port-range* • **interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/2`	Configures multiple physical ports that are connected to the DHCP clients, and enter interface range configuration mode. or Configures a single physical port that is connected to the DHCP client, and enter interface configuration mode.
Step 8	**switchport mode access** **Example:**	Defines the VLAN membership mode for the port.

	Command or Action	Purpose
	`Switch(config-if)# switchport mode access`	
Step 9	**switchport access vlan** *vlan-id* **Example:** `Switch(config-if)# switchport access vlan 1`	Assigns the ports to the same VLAN as configured in Step 2.
Step 10	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 11	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 12	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Prerequisites for Configuring DHCP Snooping and Option 82

The prerequisites for DHCP Snooping and Option 82 are as follows:

- You must globally enable DHCP snooping on the switch.
- Before globally enabling DHCP snooping on the switch, make sure that the devices acting as the DHCP server and the DHCP relay agent are configured and enabled.
- If you want the switch to respond to DHCP requests, it must be configured as a DHCP server.
- Before configuring the DHCP snooping information option on your switch, be sure to configure the device that is acting as the DHCP server. You must specify the IP addresses that the DHCP server can assign or exclude, or you must configure DHCP options for these devices.
- For DHCP snooping to function properly, all DHCP servers must be connected to the switch through trusted interfaces. In a service-provider network, a trusted interface is connected to a port on a device in the same network.
- You must configure the switch to use the Cisco IOS DHCP server binding database to use it for DHCP snooping.
- To use the DHCP snooping option of accepting packets on untrusted inputs, the switch must be an aggregation switch that receives packets with option-82 information from an edge switch.

- The following prerequisites apply to DHCP snooping binding database configuration:
  - You must configure a destination on the DHCP snooping binding database to use the switch for DHCP snooping.
  - Because both NVRAM and the flash memory have limited storage capacity, we recommend that you store the binding file on a TFTP server.
  - For network-based URLs (such as TFTP and FTP), you must create an empty file at the configured URL before the switch can write bindings to the binding file at that URL. See the documentation for your TFTP server to determine whether you must first create an empty file on the server; some TFTP servers cannot be configured this way.
  - To ensure that the lease time in the database is accurate, we recommend that you enable and configure Network Time Protocol (NTP).
  - If NTP is configured, the switch writes binding changes to the binding file only when the switch system clock is synchronized with NTP.
- Before configuring the DHCP relay agent on your switch, make sure to configure the device that is acting as the DHCP server. You must specify the IP addresses that the DHCP server can assign or exclude, configure DHCP options for devices, or set up the DHCP database agent.
- If you want the switch to relay DHCP packets, the IP address of the DHCP server must be configured on the switch virtual interface (SVI) of the DHCP client.
- If a switch port is connected to a DHCP server, configure a port as trusted by entering the **ip dhcp snooping trust interface** configuration command.
- If a switch port is connected to a DHCP client, configure a port as untrusted by entering the **no ip dhcp snooping trust** interface configuration command.

Enabling DHCP Snooping and Option 82

Follow these steps to enable DHCP snooping on the switch:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose
Step 3	**ip dhcp snooping** **Example:** `Switch(config)# ip dhcp snooping`	Enables DHCP snooping globally.
Step 4	**ip dhcp snooping vlan** *vlan-range* **Example:** `Switch(config)# ip dhcp snooping vlan 10`	Enables DHCP snooping on a VLAN or range of VLANs. The range is 1 to 4094. You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space. • You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space.
Step 5	**ip dhcp snooping information option** **Example:** `Switch(config)# ip dhcp snooping information option`	Enables the switch to insert and remove DHCP relay information (option-82 field) in forwarded DHCP request messages to the DHCP server. This is the default setting.
Step 6	**ip dhcp snooping information option format remote-id** [**string** *ASCII-string* | **hostname**] **Example:** `Switch(config)# ip dhcp snooping information option format remote-id string acsiistring2`	(Optional) Configures the remote-ID suboption. You can configure the remote ID as: • String of up to 63 ASCII characters (no spaces) • Configured hostname for the switch **Note** If the hostname is longer than 63 characters, it is truncated to 63 characters in the remote-ID configuration. The default remote ID is the switch MAC address.
Step 7	**ip dhcp snooping information option allow-untrusted** **Example:**	(Optional) If the switch is an aggregation switch connected to an edge switch, this command enables the switch to accept incoming DHCP snooping packets with option-82 information from the edge switch.

	Command or Action	Purpose
	`Switch(config)# ip dhcp snooping information option allow-untrusted`	The default setting is disabled. **Note** Enter this command only on aggregation switches that are connected to trusted devices.
Step 8	**ip dhcp snooping wireless bootp-broadcast enable (optional)** **Example:** `Switch(config)# ip dhcp snooping wireless bootp-broadcast enable`	Enables broadcast address sent by the server to be retained by the switch when it forwards DHCP packets to wireless clients.
Step 9	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet2/0/1`	Specifies the interface to be configured, and enter interface configuration mode.
Step 10	**ip dhcp snooping vlan** *vlan* **information option format-type circuit-id** [**override**] **string** *ASCII-string* **Example:** `Switch(config-if)# ip dhcp snooping vlan 1 information option format-type curcuit-id override string ovrride2`	(Optional) Configures the circuit-ID suboption for the specified interface. Specify the VLAN and port identifier, using a VLAN ID in the range of 1 to 4094. The default circuit ID is the port identifier, in the format **vlan-mod-port**. You can configure the circuit ID to be a string of 3 to 63 ASCII characters (no spaces). (Optional) Use the **override** keyword when you do not want the circuit-ID suboption inserted in TLV format to define subscriber information.
Step 11	**ip dhcp snooping trust** **Example:** `Switch(config-if)# ip dhcp snooping trust`	(Optional) Configures the interface as trusted or untrusted. Use the **no** keyword to configure an interface to receive messages from an untrusted client. The default setting is untrusted.
Step 12	**ip dhcp snooping limit rate** *rate* **Example:** `Switch(config-if)# ip dhcp snooping limit rate 100`	(Optional) Configures the number of DHCP packets per second that an interface can receive. The range is 1 to 2048. By default, no rate limit is configured.

	Command or Action	Purpose
		Note We recommend an untrusted rate limit of not more than 100 packets per second. If you configure rate limiting for trusted interfaces, you might need to increase the rate limit if the port is a trunk port assigned to more than one VLAN with DHCP snooping.
Step 13	**exit** **Example:** `Switch(config-if)# exit`	Returns to global configuration mode.
Step 14	**ip dhcp snooping verify mac-address** **Example:** `Switch(config)# ip dhcp snooping verify mac-address`	(Optional) Configures the switch to verify that the source MAC address in a DHCP packet received on untrusted ports matches the client hardware address in the packet. The default is to verify that the source MAC address matches the client hardware address in the packet.
Step 15	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 16	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 17	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Enabling the Cisco IOS DHCP Server Database

For procedures to enable and configure the Cisco IOS DHCP server database, see the “DHCP Configuration Task List” section in the “Configuring DHCP” chapter of the Cisco IOS IP Configuration Guide, Release 12.4

Monitoring DHCP Snooping Information

Table 67: Commands for Displaying DHCP Information

show ip dhcp snooping	Displays the DHCP snooping configuration for a switch
show ip dhcp snooping binding	Displays only the dynamically configured bindings in the DHCP snooping binding database, also referred to as a binding table.
show ip dhcp snooping database	Displays the DHCP snooping binding database status and statistics.
show ip dhcp snooping statistics	Displays the DHCP snooping statistics in summary or detail form.
show ip source binding	Display the dynamically and statically configured bindings.

Note If DHCP snooping is enabled and an interface changes to the down state, the switch does not delete the statically configured bindings.

Configuring DHCP Server Port-Based Address Allocation

Information About Configuring DHCP Server Port-Based Address Allocation

DHCP server port-based address allocation is a feature that enables DHCP to maintain the same IP address on an Ethernet switch port regardless of the attached device client identifier or client hardware address.

When Ethernet switches are deployed in the network, they offer connectivity to the directly connected devices. In some environments, such as on a factory floor, if a device fails, the replacement device must be working immediately in the existing network. With the current DHCP implementation, there is no guarantee that DHCP would offer the same IP address to the replacement device. Control, monitoring, and other software expect a stable IP address associated with each device. If a device is replaced, the address assignment should remain stable even though the DHCP client has changed.

When configured, the DHCP server port-based address allocation feature ensures that the same IP address is always offered to the same connected port even as the client identifier or client hardware address changes in the DHCP messages received on that port. The DHCP protocol recognizes DHCP clients by the client identifier option in the DHCP packet. Clients that do not include the client identifier option are identified by the client hardware address. When you configure this feature, the port name of the interface overrides the client identifier or hardware address and the actual point of connection, the switch port, becomes the client identifier.

In all cases, by connecting the Ethernet cable to the same port, the same IP address is allocated through DHCP to the attached device.

The DHCP server port-based address allocation feature is only supported on a Cisco IOS DHCP server and not a third-party server.

Default Port-Based Address Allocation Configuration

By default, DHCP server port-based address allocation is disabled.

Port-Based Address Allocation Configuration Guidelines

- By default, DHCP server port-based address allocation is disabled.
- To restrict assignments from the DHCP pool to preconfigured reservations (unreserved addresses are not offered to the client and other clients are not served by the pool), you can enter the **reserved-only** DHCP pool configuration command.

Enabling the DHCP Snooping Binding Database Agent

Beginning in privileged EXEC mode, follow these steps to enable and configure the DHCP snooping binding database agent on the switch:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip dhcp snooping database** {**flash**[*number*]**:**/*filename* | **ftp:**//*user***:***password***@***host*/*filename* | **http:**//[[*username***:***password*]**@**]{*hostname* | *host-ip*}[/*directory*] /*image-name***.tar** | **rcp:**//*user***@***host*/*filename*} | **tftp:**//*host*/*filename* **Example:** `Switch(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2`	Specifies the URL for the database agent or the binding file by using one of these forms: • **flash**[*number*]**:**/*filename* (Optional) Use the *number* parameter to specify the stack member number of the stack master. The range for *number* is 1 to 9. • **ftp:**//*user***:***password***@***host*/*filename* • **http:**//[[*username***:***password*]**@**]{*hostname* | *host-ip*}[/*directory*] /*image-name***.tar** • **rcp:**//*user***@***host*/*filename*

	Command or Action	Purpose
		• **tftp:**//*host*/*filename*
Step 4	**ip dhcp snooping database timeout** *seconds* **Example:** `Switch(config)# ip dhcp snooping database timeout 300`	Specifies (in seconds) how long to wait for the database transfer process to finish before stopping the process. The default is 300 seconds. The range is 0 to 86400. Use 0 to define an infinite duration, which means to continue trying the transfer indefinitely.
Step 5	**ip dhcp snooping database write-delay** *seconds* **Example:** `Switch(config)# ip dhcp snooping database write-delay 15`	Specifies the duration for which the transfer should be delayed after the binding database changes. The range is from 15 to 86400 seconds. The default is 300 seconds (5 minutes).
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	**ip dhcp snooping binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* **expiry** *seconds* **Example:** `Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000`	(Optional) Adds binding entries to the DHCP snooping binding database. The *vlan-id* range is from 1 to 4904. The *seconds* range is from 1 to 4294967295. Enter this command for each entry that you add. Use this command when you are testing or debugging the switch.
Step 8	**show ip dhcp snooping database** [**detail**] **Example:** `Switch# show ip dhcp snooping database detail`	Displays the status and statistics of the DHCP snooping binding database agent.
Step 9	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 10	**copy running-config startup-config** **Example:** `Switch# copy running-config`	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	`startup-config`	

Enabling DHCP Server Port-Based Address Allocation

Follow these steps to globally enable port-based address allocation and to automatically generate a subscriber identifier on an interface.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip dhcp use subscriber-id client-id** **Example:** `Switch(config)# ip dhcp use subscriber-id client-id`	Configures the DHCP server to globally use the subscriber identifier as the client identifier on all incoming DHCP messages.
Step 4	**ip dhcp subscriber-id interface-name** **Example:** `Switch(config)# ip dhcp subscriber-id interface-name`	Automatically generates a subscriber identifier based on the short name of the interface. A subscriber identifier configured on a specific interface takes precedence over this command.
Step 5	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/1`	Specifies the interface to be configured, and enter interface configuration mode.
Step 6	**ip dhcp server use subscriber-id client-id** **Example:** `Switch(config-if)# ip dhcp server use subscriber-id client-id`	Configures the DHCP server to use the subscriber identifier as the client identifier on all incoming DHCP messages on the interface.

	Command or Action	Purpose
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 8	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 9	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

After enabling DHCP port-based address allocation on the switch, use the **ip dhcp pool** global configuration command to preassign IP addresses and to associate them to clients.

Monitoring DHCP Server Port-Based Address Allocation

Table 68: Commands for Displaying DHCP Port-Based Address Allocation Information

Command	Purpose
show interface *interface id*	Displays the status and configuration of a specific interface.
show ip dhcp pool	Displays the DHCP address pools.
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.

Additional References

Related Documents

Related Topic	Document Title
DHCP Configuration Information and Procedures	IP Addressing: DHCP Configuration Guide, Cisco IOS XE Release 3S http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3s/dhcp-xe-3s-book.html

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

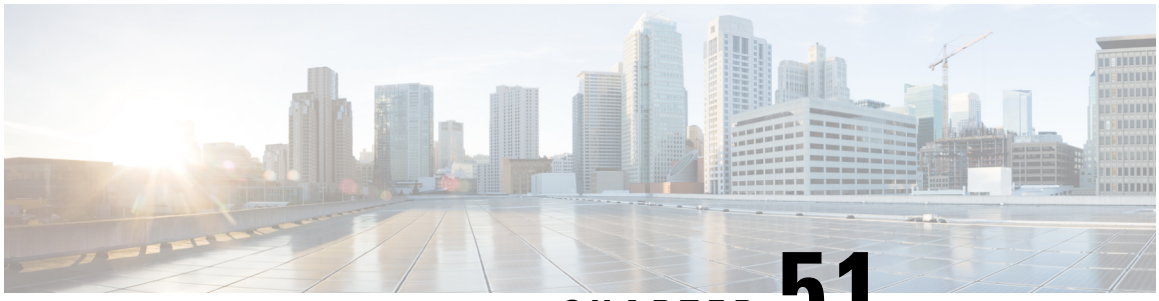
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for DHCP Snooping and Option 82

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.

Release	Feature Information
	Introduced support for the following commands: • **show ip dhcp snooping statistics** user EXEC command for displaying DHCP snooping statistics. • **clear ip dhcp snooping statistics** privileged EXEC command for clearing the snooping statistics counters.



CHAPTER 51

Configuring IP Source Guard

IP Source Guard (IPSG) is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings.

This chapter contains the following topics:

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IP Source Guard

IP Source Guard

You can use IP source guard to prevent traffic attacks if a host tries to use the IP address of its neighbor and you can enable IP source guard when DHCP snooping is enabled on an untrusted interface.

After IPSG is enabled on an interface, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping.

The switch uses a source IP lookup table in hardware to bind IP addresses to ports. For IP and MAC filtering, a combination of source IP and source MAC lookups are used. IP traffic with a source IP address is the binding table is allowed, all other traffic is denied.

The IP source binding table has bindings that are learned by DHCP snooping or are manually configured (static IP source bindings). An entry in this table has an IP address, its associated MAC address, and its associated VLAN number. The switch uses the IP source binding table only when IP source guard is enabled.

IPSG is supported only on Layer 2 ports, including access and trunk ports. You can configure IPSG with source IP address filtering or with source IP and MAC address filtering.

IP Source Guard for Static Hosts

Note Do not use IPSG (IP source guard) for static hosts on uplink ports or trunk ports.

IPSG for static hosts extends the IPSG capability to non-DHCP and static environments. The previous IPSG used the entries created by DHCP snooping to validate the hosts connected to a switch. Any traffic received from a host without a valid DHCP binding entry is dropped. This security feature restricts IP traffic on nonrouted Layer 2 interfaces. It filters traffic based on the DHCP snooping binding database and on manually configured IP source bindings. The previous version of IPSG required a DHCP environment for IPSG to work.

IPSG for static hosts allows IPSG to work without DHCP. IPSG for static hosts relies on IP device tracking-table entries to install port ACLs. The switch creates static entries based on ARP requests or other IP packets to maintain the list of valid hosts for a given port. You can also specify the number of hosts allowed to send traffic to a given port. This is equivalent to port security at Layer 3.

IPSG for static hosts also supports dynamic hosts. If a dynamic host receives a DHCP-assigned IP address that is available in the IP DHCP snooping table, the same entry is learned by the IP device tracking table. In a stacked environment, when the master failover occurs, the IP source guard entries for static hosts attached to member ports are retained. When you enter the **show ip device tracking all** EXEC command, the IP device tracking table displays the entries as ACTIVE.

Note Some IP hosts with multiple network interfaces can inject some invalid packets into a network interface. The invalid packets contain the IP or MAC address for another network interface of the host as the source address. The invalid packets can cause IPSG for static hosts to connect to the host, to learn the invalid IP or MAC address bindings, and to reject the valid bindings. Consult the vender of the corresponding operating system and the network interface to prevent the host from injecting invalid packets.

IPSG for static hosts initially learns IP or MAC bindings dynamically through an ACL-based snooping mechanism. IP or MAC bindings are learned from static hosts by ARP and IP packets. They are stored in the device tracking database. When the number of IP addresses that have been dynamically learned or statically configured on a given port reaches a maximum, the hardware drops any packet with a new IP address. To resolve hosts that have moved or gone away for any reason, IPSG for static hosts leverages IP device tracking to age out dynamically learned IP address bindings. This feature can be used with DHCP snooping. Multiple bindings are established on a port that is connected to both DHCP and static hosts. For example, bindings are stored in both the device tracking database as well as in the DHCP snooping binding database.

IP Source Guard Configuration Guidelines

- You can configure static IP bindings only on nonrouted ports. If you enter the **ip source binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* global configuration command on a routed interface, this error message appears:

```
Static IP source binding can only be configured on switch port.
```

- When IP source guard with source IP filtering is enabled on an interface, DHCP snooping must be enabled on the access VLAN for that interface.
- If you are enabling IP source guard on a trunk interface with multiple VLANs and DHCP snooping is enabled on all the VLANs, the source IP address filter is applied on all the VLANs.

Note If IP source guard is enabled and you enable or disable DHCP snooping on a VLAN on the trunk interface, the switch might not properly filter traffic.

- You can enable this feature when 802.1x port-based authentication is enabled.
- When you configure IP source guard smart logging, packets with a source address other than the specified address or an address learned by DHCP are denied, and the packet contents are sent to a NetFlow collector. If you configure this feature, make sure that smart logging is globally enabled.
- In a switch stack, if IP source guard is configured on a stack member interface and you remove the the configuration of that switch by entering the **no switch** *stack-member-number* **provision** global configuration command, the interface static bindings are removed from the binding table, but they are not removed from the running configuration. If you again provision the switch by entering the **switch** *stack-member-number* **provision** command, the binding is restored.

  To remove the binding from the running configuration, you must disable IP source guard before entering the **no switch provision** command. The configuration is also removed if the switch reloads while the interface is removed from the binding table.

How to Configure IP Source Guard

Enabling IP Source Guard

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Specifies the interface to be configured, and enters interface configuration mode.
Step 4	**ip verify source** [**mac-check**] **Example:** `Switch(config-if)# ip verify source`	Enables IP source guard with source IP address filtering. (Optional) **mac-check**—Enables IP Source Guard with source IP address and MAC address filtering.
Step 5	**exit** **Example:** `Switch(config-if)# exit`	Returns to global configuration mode.
Step 6	**ip source binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* **Example:** `Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1`	Adds a static IP source binding. Enter this command for each static binding.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 8	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 9	**copy running-config startup-config** **Example:**	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	`Switch# copy running-config startup-config`	

Configuring IP Source Guard for Static Hosts on a Layer 2 Access Port

You must configure the **ip device tracking maximum** *limit-number* interface configuration command globally for IPSG for static hosts to work. If you only configure this command on a port without enabling IP device tracking globally or by setting an IP device tracking maximum on that interface, IPSG with static hosts rejects all the IP traffic from that interface.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip device tracking** **Example:** `Switch(config)# ip device tracking`	Turns on the IP host table, and globally enables IP device tracking.
Step 4	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Enters interface configuration mode.
Step 5	**switchport mode access** **Example:** `Switch(config-if)# switchport mode access`	Configures a port as access.

	Command or Action	Purpose
Step 6	**switchport access vlan** *vlan-id* **Example:** `Switch(config-if)# switchport access vlan 10`	Configures the VLAN for this port.
Step 7	**ip device tracking maximum** *number* **Example:** `Switch(config-if)# ip device tracking maximum 8`	Establishes a maximum limit for the number of static IPs that the IP device tracking table allows on the port. The range is 1to 10. The maximum number is 10. **Note** You must configure the **ip device tracking maximum** *limit-number* interface configuration command.
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Monitoring IP Source Guard

Table 69: Privileged EXEC show Commands

Command	Purpose
show ip verify source [**interface** *interface-id*]	Displays the IP source guard configuration on the switch or on a specific interface.
show ip device tracking { **all** | **interface** *interface-id* | **ip** *ip-address* | **mac** *imac-address*}	Displays information about the entries in the IP device tracking table.

Table 70: Interface Configuration Commands

Command	Purpose
ip verify source tracking	Verifies the data source.

For detailed information about the fields in these displays, see the command reference for this release.

Additional References

Error Message Decoder

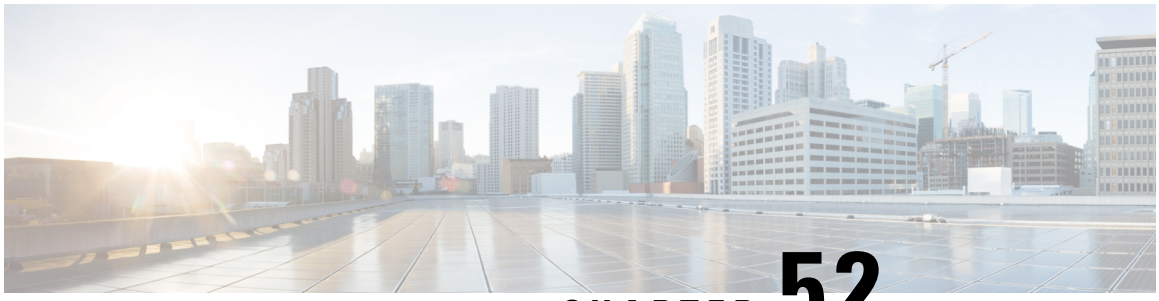
Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support



CHAPTER 52

Configuring Dynamic ARP Inspection

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Dynamic ARP Inspection

This section lists the restrictions and guidelines for configuring Dynamic ARP Inspection on the switch.

- Dynamic ARP inspection is an ingress security feature; it does not perform any egress checking.
- Dynamic ARP inspection is not effective for hosts connected to switches that do not support dynamic ARP inspection or that do not have this feature enabled. Because man-in-the-middle attacks are limited to a single Layer 2 broadcast domain, separate the domain with dynamic ARP inspection checks from the one with no checking. This action secures the ARP caches of hosts in the domain enabled for dynamic ARP inspection.

- Dynamic ARP inspection depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically assigned IP addresses.

  When DHCP snooping is disabled or in non-DHCP environments, use ARP ACLs to permit or to deny packets.

- Dynamic ARP inspection is supported on access ports, trunk ports, and EtherChannel ports.

  Note Do not enable Dynamic ARP inspection on RSPAN VLANs. If Dynamic ARP inspection is enabled on RSPAN VLANs, Dynamic ARP inspection packets might not reach the RSPAN destination port.

- A physical port can join an EtherChannel port channel only when the trust state of the physical port and the channel port match. Otherwise, the physical port remains suspended in the port channel. A port channel inherits its trust state from the first physical port that joins the channel. Consequently, the trust state of the first physical port need not match the trust state of the channel.

  Conversely, when you change the trust state on the port channel, the switch configures a new trust state on all the physical ports that comprise the channel.

- The rate limit is calculated separately on each switch in a switch stack. For a cross-stack EtherChannel, this means that the actual rate limit might be higher than the configured value. For example, if you set the rate limit to 30 pps on an EtherChannel that has one port on switch 1 and one port on switch 2, each port can receive packets at 29 pps without causing the EtherChannel to become error-disabled.

- The operating rate for the port channel is cumulative across all the physical ports within the channel. For example, if you configure the port channel with an ARP rate-limit of 400 pps, all the interfaces combined on the channel receive an aggregate 400 pps. The rate of incoming ARP packets on EtherChannel ports is equal to the sum of the incoming rate of packets from all the channel members. Configure the rate limit for EtherChannel ports only after examining the rate of incoming ARP packets on the channel-port members.

  The rate of incoming packets on a physical port is checked against the port-channel configuration rather than the physical-ports configuration. The rate-limit configuration on a port channel is independent of the configuration on its physical ports.

  If the EtherChannel receives more ARP packets than the configured rate, the channel (including all physical ports) is placed in the error-disabled state.

- Make sure to limit the rate of ARP packets on incoming trunk ports. Configure trunk ports with higher rates to reflect their aggregation and to handle packets across multiple dynamic ARP inspection-enabled VLANs. You also can use the **ip arp inspection limit none** interface configuration command to make the rate unlimited. A high rate-limit on one VLAN can cause a denial-of-service attack to other VLANs when the software places the port in the error-disabled state.

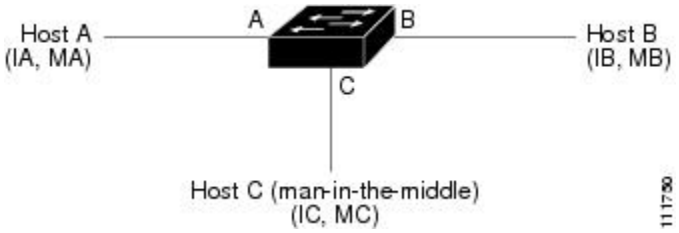
- When you enable dynamic ARP inspection on the switch, policers that were configured to police ARP traffic are no longer effective. The result is that all ARP traffic is sent to the CPU.

Understanding Dynamic ARP Inspection

ARP provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. For example, Host B wants to send information to Host A but does not have the MAC address of Host A in its ARP cache. Host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of Host A. All hosts within the broadcast domain receive the ARP request, and Host A responds with its MAC address. However,because ARP allows a gratuitous reply from a host even if an ARP request was not received, an ARP spoofing attack and the poisoning of ARP caches can occur. After the attack, all traffic from the device under attack flows through the attacker's computer and then to the router, switch, or host.

A malicious user can attack hosts, switches, and routers connected to your Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet. Figure 26-1 shows an example of ARP cache poisoning.

Figure 56: ARP Cache Poisoning



Hosts A, B, and C are connected to the switch on interfaces A, B and C, all of which are on the same subnet. Their IP and MAC addresses are shown in parentheses; for example, Host A uses IP address IA and MAC address MA. When Host A needs to communicate to Host B at the IP layer, it broadcasts an ARP request for the MAC address associated with IP address IB. When the switch and Host B receive the ARP request, they populate their ARP caches with an ARP binding for a host with the IP address IA and a MAC address MA; for example, IP address IA is bound to MAC address MA. When Host B responds, the switch and Host A populate their ARP caches with a binding for a host with the IP address IB and the MAC address MB.

Host C can poison the ARP caches of the switch, Host A, and Host B by broadcasting forged ARP responses with bindings for a host with an IP address of IA (or IB) and a MAC address of MC. Hosts with poisoned ARP caches use the MAC address MC as the destination MAC address for traffic intended for IA or IB. This means that Host C intercepts that traffic. Because Host C knows the true MAC addresses associated with IA and IB, it can forward the intercepted traffic to those hosts by using the correct MAC address as the destination. Host C has inserted itself into the traffic stream from Host A to Host B, the classic *man-in-the middle*attack.

Dynamic ARP inspection is a security feature that validates ARP packets in a network. It intercepts, logs,and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.

Dynamic ARP inspection ensures that only valid ARP requests and responses are relayed. The switch performs these activities:

- Intercepts all ARP requests and responses on untrusted ports
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination
- Drops invalid ARP packets

Dynamic ARP inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid.

You enable dynamic ARP inspection on a per-VLAN basis by using the **ip arp inspection vlan** *vlan-range* global configuration command.

In non-DHCP environments, dynamic ARP inspection can validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses. You define an ARP ACL by using the **arp access-list** *acl-name* global configuration command.

You can configure dynamic ARP inspection to drop ARP packets when the IP addresses in the packets are invalid or when the MAC addresses in the body of the ARP packets do not match the addresses specified in the Ethernet header. Use the **ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} global configuration command.

Interface Trust States and Network Security

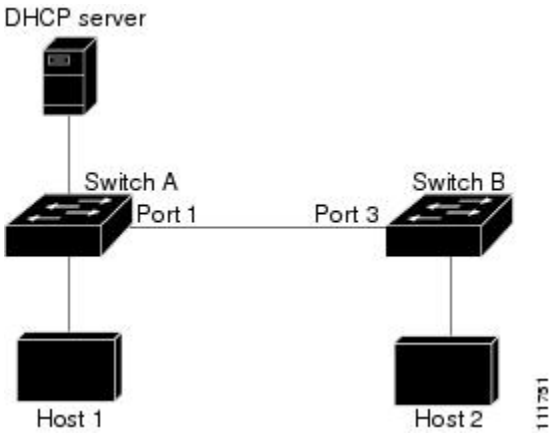
Dynamic ARP inspection associates a trust state with each interface on the switch. Packets arriving on trusted interfaces bypass all dynamic ARP inspection validation checks, and those arriving on untrusted interfaces undergo the dynamic ARP inspection validation process.

In a typical network configuration, you configure all switch ports connected to host ports as untrusted and configure all switch ports connected to switches as trusted. With this configuration, all ARP packets entering the network from a given switch bypass the security check. No other validation is needed at any other place in the VLAN or in the network. You configure the trust setting by using theip arp inspection trust interface configuration command.

Caution Use the trust state configuration carefully. Configuring interfaces as untrusted when they should betrusted can result in a loss of connectivity.

In the following figure, assume that both Switch A and Switch B are running dynamic ARP inspection on the VLAN that includes Host 1 and Host 2. If Host 1 and Host 2 acquire their IP addresses from the DHCP server connected to Switch A, only Switch A binds the IP-to-MAC address of Host 1. Therefore, if the interface between Switch A and Switch B is untrusted, the ARP packets from Host 1 are dropped by Switch B. Connectivity between Host 1 and Host 2 is lost.

Figure 57: ARP Packet Validation on a VLAN Enabled for Dynamic ARP Inspection



Configuring interfaces to be trusted when they are actually untrusted leaves a security hole in the network. If Switch A is not running dynamic ARP inspection, Host 1 can easily poison the ARP cache of Switch B (and Host 2, if the link between the switches is configured as trusted). This condition can occur even though Switch B is running dynamic ARP inspection.

Dynamic ARP inspection ensures that hosts (on untrusted interfaces) connected to a switch running dynamic ARP inspection do not poison the ARP caches of other hosts in the network. However, dynamic ARP inspection does not prevent hosts in other portions of the network from poisoning the caches of the hosts that are connected to a switch running dynamic ARP inspection.

In cases in which some switches in a VLAN run dynamic ARP inspection and other switches do not, configure the interfaces connecting such switches as untrusted. However, to validate the bindings of packets from nondynamic ARP inspection switches, configure the switch running dynamic ARP inspection with ARP ACLs. When you cannot determine such bindings, at Layer 3, isolate switches running dynamic ARP inspection from switches not running dynamic ARP inspection switches.

Note Depending on the setup of the DHCP server and the network, it might not be possible to validate a given ARP packet on all switches in the VLAN.

Rate Limiting of ARP Packets

The switch CPU performs dynamic ARP inspection validation checks; therefore, the number of incoming ARP packets is rate-limited to prevent a denial-of-service attack. By default, the rate for untrusted interfaces is 15 packets per second (pps). Trusted interfaces are not rate-limited. You can change this setting by using the **ip arp inspection limit** interface configuration command.

When the rate of incoming ARP packets exceeds the configured limit, the switch places the port in the error-disabled state. The port remains in that state until you intervene. You can use the **errdisable recovery** global configuration command to enable error disable recovery so that ports automatically emerge from this state after a specified timeout period.

Note The rate limit for an EtherChannel is applied separately to each switch in a stack. For example, if a limit of 20 pps is configured on the EtherChannel, each switch with ports in the EtherChannel can carry up to 20 pps. If any switch exceeds the limit, the entire EtherChannel is placed into the error-disabled state.

Relative Priority of ARP ACLs and DHCP Snooping Entries

Dynamic ARP inspection uses the DHCP snooping binding database for the list of valid IP-to-MAC address bindings.

ARP ACLs take precedence over entries in the DHCP snooping binding database. The switch uses ACLs only if you configure them by using the **ip arp inspection filter vlan** global configuration command. The switch first compares ARP packets to user-configured ARP ACLs. If the ARP ACL denies the ARP packet, the switch also denies the packet even if a valid binding exists in the database populated by DHCP snooping.

Logging of Dropped Packets

When the switch drops a packet, it places an entry in the log buffer and then generates system messages on a rate-controlled basis. After the message is generated, the switch clears the entry from the log buffer. Each log entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.

You use the **ip arp inspection log-buffer** global configuration command to configure the number of entries in the buffer and the number of entries needed in the specified interval to generate system messages. You specify the type of packets that are logged by using the **ip arp inspection vlan logging** global configuration command.

Default Dynamic ARP Inspection Configuration

Feature	Default Settings
Dynamic ARP inspection	Disabled on all VLANs.
Interface trust state	All interfaces are untrusted.
Rate limit of incoming ARP packets	The rate is 15 pps on untrusted interfaces, assuming that the network is a switched network with a host connecting to as many as 15 new hosts per second. The rate is unlimited on all trusted interfaces. The burst interval is 1 second.
ARP ACLs for non-DHCP environments	No ARP ACLs are defined.
Validation checks	No checks are performed.

Feature	Default Settings
Log buffer	When dynamic ARP inspection is enabled, all denied or dropped ARP packets are logged. The number of entries in the log is 32. The number of system messages is limited to 5 per second. The logging-rate interval is 1 second.
Per-VLAN logging	All denied or dropped ARP packets are logged.

Relative Priority of ARP ACLs and DHCP Snooping Entries

Dynamic ARP inspection uses the DHCP snooping binding database for the list of valid IP-to-MAC address bindings.

ARP ACLs take precedence over entries in the DHCP snooping binding database. The switch uses ACLs only if you configure them by using the ip arp inspection filter vlan global configuration command. The switch first compares ARP packets to user-configured ARP ACLs. If the ARP ACL denies the ARP packet, the switch also denies the packet even if a valid binding exists in the database populated by DHCP snooping.

Configuring ARP ACLs for Non-DHCP Environments

This procedure shows how to configure dynamic ARP inspection when Switch B shown in Figure 2 does not support dynamic ARP inspection or DHCP snooping.

If you configure port 1 on Switch A as trusted, a security hole is created because both Switch A and Host 1 could be attacked by either Switch B or Host 2. To prevent this possibility, you must configure port 1 on Switch A as untrusted. To permit ARP packets from Host 2, you must set up an ARP ACL and apply it to VLAN 1. If the IP address of Host 2 is not static (it is impossible to apply the ACL configuration on Switch A) you must separate Switch A from Switch B at Layer 3 and use a router to route packets between them.

Follow these steps to configure an ARP ACL on Switch A. This procedure is required in non-DHCP environments.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters the global configuration mode.

	Command or Action	Purpose
	`Switch# configure terminal`	
Step 3	**arp access-list** *acl-name*	Defines an ARP ACL, and enters ARP access-list configuration mode. By default, no ARP access lists are defined. **Note** At the end of the ARP access list, there is an implicit **deny ip any mac any** command.
Step 4	**permit ip host** *sender-ip* **mac host** *sender-mac*	Permits ARP packets from the specified host (Host 2). • For*sender-ip*, enter the IP address of Host 2. • For *sender-mac*, enter the MAC address of Host 2.
Step 5	**exit**	Returns to global configuration mode.
Step 6	**ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* [**static**]	Applies ARP ACL to the VLAN. By default, no defined ARP ACLs are applied to any VLAN. • For *arp-acl-name*, specify the name of the ACL created in Step 2. • For *vlan-range*, specify the VLAN that the switches and hosts are in. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. • (Optional) Specify **static** to treat implicit denies in the ARP ACL as explicit denies and to drop packets that do not match any previous clauses in the ACL. DHCP bindings are not used. If you do not specify this keyword, it means that there is no explicit deny in the ACL that denies the packet, and DHCP bindings determine whether a packet is permitted or denied if the packet does not match any clauses in the ACL. ARP packets containing only IP-to-MAC address bindings are compared against the

	Command or Action	Purpose
		ACL. Packets are permitted only if the access list permits them.
Step 7	**interface** *interface-id*	Specifies Switch A interface that is connected to Switch B, and enters the interface configuration mode.
Step 8	**no ip arp inspection trust**	Configures Switch A interface that is connected to Switch B as untrusted. By default, all interfaces are untrusted. For untrusted interfaces, the switch intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The switch drops invalid packets and logs them in the log buffer according to the logging configuration specified with the **ip arp inspection vlan logging** global configuration command.
Step 9	**end**	Returns to privileged EXEC mode.
Step 10	Use the following show commands: • **show arp access-list** acl-name • **show ip arp inspection vlan** *vlan-range* • **show ip arp inspection interfaces**	Verifies your entries.
Step 11	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 12	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Dynamic ARP Inspection in DHCP Environments

Before you begin

This procedure shows how to configure dynamic ARP inspection when two switches support this feature. Host 1 is connected to Switch A, and Host 2 is connected to Switch B. Both switches are running dynamic

ARP inspection on VLAN 1 where the hosts are located. A DHCP server is connected to Switch A. Both hosts acquire their IP addresses from the same DHCP server. Therefore, Switch A has the bindings for Host 1 and Host 2, and Switch B has the binding for Host 2.

Note Dynamic ARP inspection depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically assigned IP addresses.

Follow these steps to configure dynamic ARP inspection. You must perform this procedure on both switches. This procedure is required.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show cdp neighbors** **Example:** `Switch(config-if)#show cdp neighbors`	Verify the connection between the switches.
Step 3	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 4	**ip arp inspection vlan** *vlan-range* **Example:** `Switch(config)# ip arp inspection vlan 1`	Enable dynamic ARP inspection on a per-VLAN basis. By default, dynamic ARP inspection is disabled on all VLANs. For vlan-range, specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. Specify the same VLAN ID for both switches.
Step 5	**Interface***interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/1`	Specifies the interface connected to the other switch, and enter interface configuration mode.
Step 6	**ip arp inspection trust** **Example:** `Switch(config-if)#ip arp inspection trust`	Configures the connection between the switches as trusted. By default, all interfaces are untrusted.

	Command or Action	Purpose
		The switch does not check ARP packets that it receives from the other switch on the trusted interface. It simply forwards the packets. For untrusted interfaces, the switch intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The switch drops invalid packets and logs them in the log buffer according to the logging configuration specified with the ip arp inspection vlan logging global configuration command.
Step 7	**end** **Example:** `Switch(config-if)#end`	Returns to privileged EXEC mode.
Step 8	**show ip arp inspection interfaces** **Example:**	Verifies the dynamic ARP inspection configuration on interfaces.
Step 9	**show ip arp inspection vlan** *vlan-range* **Example:** `Switch(config-if)#show ip arp inspection vlan 1`	Verifies the dynamic ARP inspection configuration on VLAN.
Step 10	**show ip dhcp snooping binding** **Example:** `Switch(config-if)#show ip dhcp snooping binding`	Verifies the DHCP bindings.
Step 11	**show ip arp inspection statistics vlan** *vlan-range* **Example:** `Switch(config-if)#show ip arp inspection statistics vlan 1`	Checks the dynamic ARP inspection statistics on VLAN.
Step 12	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 13	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

Limiting the Rate of Incoming ARP Packets

The switch CPU performs dynamic ARP inspection validation checks; therefore, the number of incoming ARP packets is rate-limited to prevent a denial- of-service attack.

When the rate of incoming ARP packets exceeds the configured limit, the switch places the port in the error-disabled state. The port remains in that state until you enable error-disabled recovery so that ports automatically emerge from this state after a specified timeout period.

Note Unless you configure a rate limit on an interface, changing the trust state of the interface also changes its rate limit to the default value for that trust state. After you configure the rate limit, the interface retains the rate limit even when its trust state is changed. If you enter the **no ip arp inspection limit** interface configuration command, the interface reverts to its default rate limit.

Follow these steps to limit the rate of incoming ARP packets. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id*	Specifies the interface to be rate-limited, and enter interface configuration mode.
Step 4	**ip arp inspection limit {rate pps [burst interval seconds] | none}**	Limits the rate of incoming ARP requests and responses on the interface. The default rate is 15 pps on untrusted interfaces and unlimited on trusted interfaces. The burst interval is 1 second. The keywords have these meanings: • For **rate***pps*, specify an upper limit for the number of incoming packets processed per second. The range is 0 to 2048 pps. • (Optional) For **burst interval***seconds*, specify the consecutive interval in

	Command or Action	Purpose
		seconds, over which the interface is monitored for a high rate of ARP packets. The range is 1 to 15. • For **rate none**, specify no upper limit for the rate of incoming ARP packets that can be processed.
Step 5	**exit**	Returns to global configuration mode.
Step 6	Use the following commands: • **errdisable detect cause arp-inspection** • **errdisable recovery cause arp-inspection** • **errdisable recovery interval** *interval*	(Optional) Enables error recovery from the dynamic ARP inspection error-disabled state, and configure the dynamic ARP inspection recover mechanism variables. By default, recovery is disabled, and the recovery interval is 300 seconds. For **interval** *interval*, specify the time in seconds to recover from the error-disabled state. The range is 30 to 86400.
Step 7	**exit**	Returns to privileged EXEC mode.
Step 8	Use the following show commands: • **show ip arp inspection interfaces** • **show errdisable recovery**	Verifies your settings.
Step 9	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 10	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Performing Dynamic ARP Inspection Validation Checks

Dynamic ARP inspection intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. You can configure the switch to perform additional checks on the destination MAC address, the sender and target IP addresses, and the source MAC address.

Follow these steps to perform specific checks on incoming ARP packets. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip arp inspection validate {[src-mac] [dst-mac] [ip]}**	Performs a specific check on incoming ARP packets. By default, no checks are performed. The keywords have these meanings: • For **src-mac**, check the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped. • For **dst-mac**, check the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped. • For **ip**, check the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses. You must specify at least one of the keywords. Each command overrides the configuration of the previous command; that is, if a command enables src and dst mac validations, and a second command enables IP validation only, the src and dst mac validations are disabled as a result of the second command.
Step 4	**exit**	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	**show ip arp inspection vlan** *vlan-range*	Verifies your settings.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Monitoring DAI

To monitor DAI, use the following commands:

Command	Description
clear ip arp inspection statistics	Clears dynamic ARP inspection statistics.
show ip arp inspection statistics [**vlan** *vlan-range*]	Displays statistics for forwarded, dropped, MAC validation failure, IP validation failure, ACL permitted and denied, and DHCP permitted and denied packets for the specified VLAN. If no VLANs are specified or if a range is specified, displays information only for VLANs with dynamic ARP inspection enabled (active).
clear ip arp inspection log	Clears the dynamic ARP inspection log buffer.
show ip arp inspection log	Displays the configuration and contents of the dynamic ARP inspection log buffer.

For the **show ip arp inspection statistics** command, the switch increments the number of forwarded packets for each ARP request and response packet on a trusted dynamic ARP inspection port. The switch increments the number of ACL or DHCP permitted packets for each packet that is denied by source MAC, destination MAC, or IP validation checks, and the switch increments the appropriate.

Verifying the DAI Configuration

To display and verify the DAI configuration, use the following commands:

Command	Description
show arp access-list [*acl-name*]	Displays detailed information about ARP ACLs.

Command	Description
show ip arp inspection interfaces [interface-id]	Displays the trust state and the rate limit of ARP packets for the specified interface or all interfaces.
show ip arp inspection vlan *vlan-range*	Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN. If no VLANs are specified or if a range is specified, displays information only for VLANs with dynamic ARP inspection enabled (active).

Additional References

Error Message Decoder

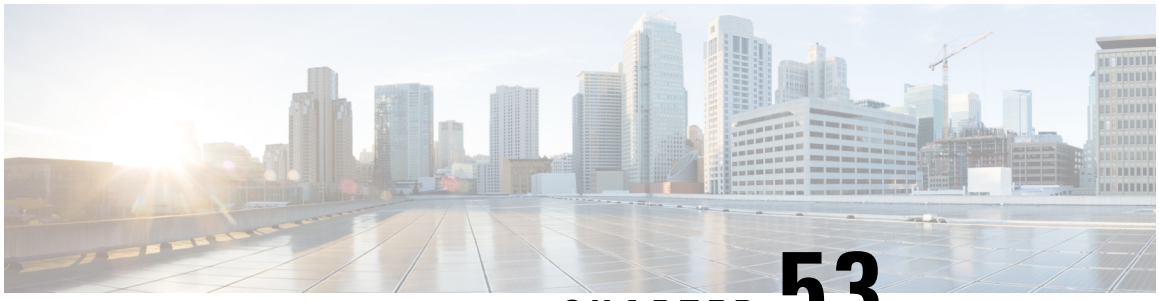
Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support



CHAPTER 53

Configuring IEEE 802.1x Port-Based Authentication

This chapter describes how to configure IEEE 802.1x port-based authentication. IEEE 802.1x authentication prevents unauthorized devices (clients) from gaining access to the network. Unless otherwise noted, the term *switch* refers to a standalone switch or a switch stack.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About 802.1x Port-Based Authentication

The 802.1x standard defines a client-server-based access control and authentication protocol that prevents unauthorized clients from connecting to a LAN through publicly accessible ports unless they are properly authenticated. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

Note TACACS is not supported with 802.1x authentication.

Until the client is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

The table shown below lists the maximum number of each client session supported on Catalyst 3850 and Catalyst 3650 switches:

Client session	Maximum sessions supported
Maximum dot1x or MAB client sessions	2000
Maximum web-based authentication sessions	2000
Maximum dot1x sessions with critical-auth VLAN enabled and server re-initialized	2000
Maximum MAB sessions with various session features applied	2000
Maximum dot1x sessions with service templates or session features applied	2000

Note For complete syntax and usage information for the commands used in this chapter, see the "RADIUS Commands" section in the *Cisco IOS Security Command Reference, Release 3SE*

Port-Based Authentication Process

To configure IEEE 802.1X port-based authentication, you must enable authentication, authorization, and accounting (AAA) and specify the authentication method list. A method list describes the sequence and authentication method to be queried to authenticate a user.

The AAA process begins with authentication. When 802.1x port-based authentication is enabled and the client supports 802.1x-compliant client software, these events occur:

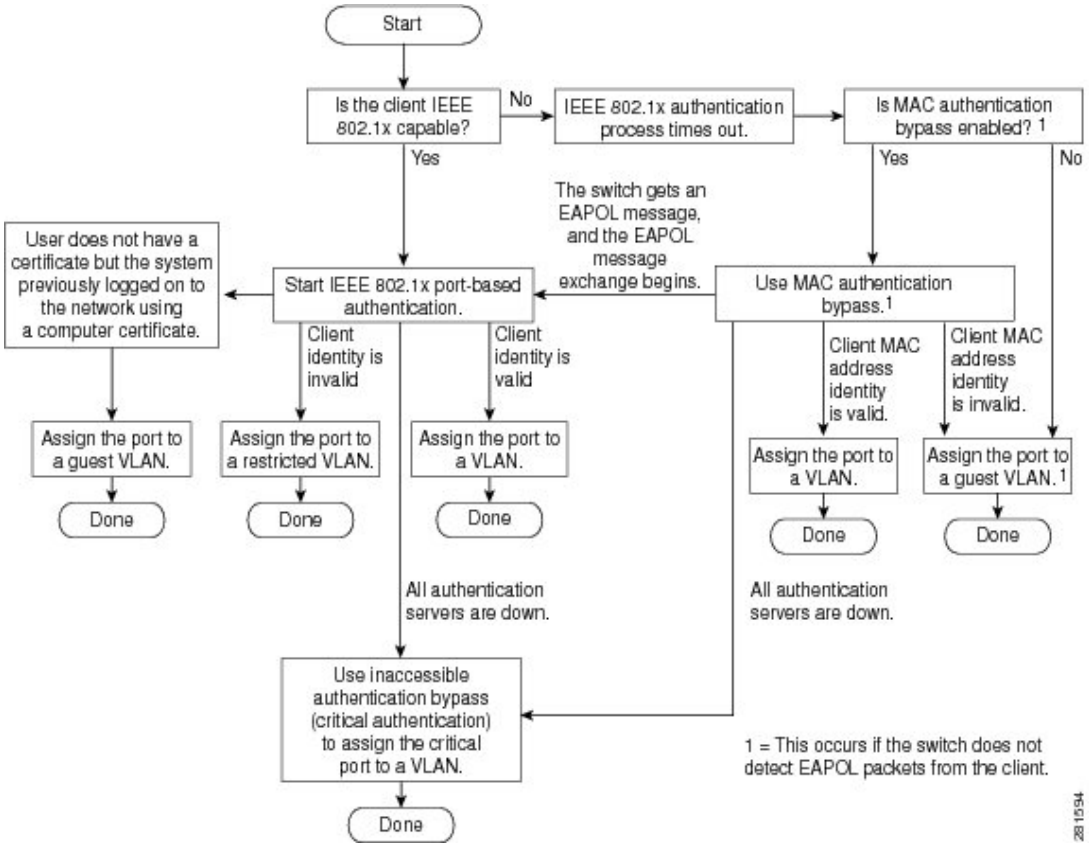
- If the client identity is valid and the 802.1x authentication succeeds, the switch grants the client access to the network.
- If 802.1x authentication times out while waiting for an EAPOL message exchange and MAC authentication bypass is enabled, the switch can use the client MAC address for authorization. If the client MAC address is valid and the authorization succeeds, the switch grants the client access to the network. If the client MAC address is invalid and the authorization fails, the switch assigns the client to a guest VLAN that provides limited services if a guest VLAN is configured.
- If the switch gets an invalid identity from an 802.1x-capable client and a restricted VLAN is specified, the switch can assign the client to a restricted VLAN that provides limited services.
- If the RADIUS authentication server is unavailable (down) and inaccessible authentication bypass is enabled, the switch grants the client access to the network by putting the port in the critical-authentication state in the RADIUS-configured or the user-specified access VLAN.

Note Inaccessible authentication bypass is also referred to as critical authentication or the AAA fail policy.

If Multi Domain Authentication (MDA) is enabled on a port, this flow can be used with some exceptions that are applicable to voice authorization.

Figure 58: Authentication Flowchart

This figure shows the authentication process.



The switch re-authenticates a client when one of these situations occurs:

- Periodic re-authentication is enabled, and the re-authentication timer expires.

  You can configure the re-authentication timer to use a switch-specific value or to be based on values from the RADIUS server.

  After 802.1x authentication using a RADIUS server is configured, the switch uses timers based on the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute [29]).

  The Session-Timeout RADIUS attribute (Attribute[27]) specifies the time after which re-authentication occurs.

  The Termination-Action RADIUS attribute (Attribute [29]) specifies the action to take during re-authentication. The actions are *Initialize* and *ReAuthenticate*. When the *Initialize* action is set (the

attribute value is *DEFAULT*), the 802.1x session ends, and connectivity is lost during re-authentication. When the *ReAuthenticate* action is set (the attribute value is RADIUS-Request), the session is not affected during re-authentication.

- You manually re-authenticate the client by entering the **dot1x re-authenticate interface** *interface-id* privileged EXEC command.

Port-Based Authentication Initiation and Message Exchange

During 802.1x authentication, the switch or the client can initiate authentication. If you enable authentication on a port by using the **authentication port-control auto** interface configuration command, the switch initiates authentication when the link state changes from down to up or periodically as long as the port remains up and unauthenticated. The switch sends an EAP-request/identity frame to the client to request its identity. Upon receipt of the frame, the client responds with an EAP-response/identity frame.

However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity.

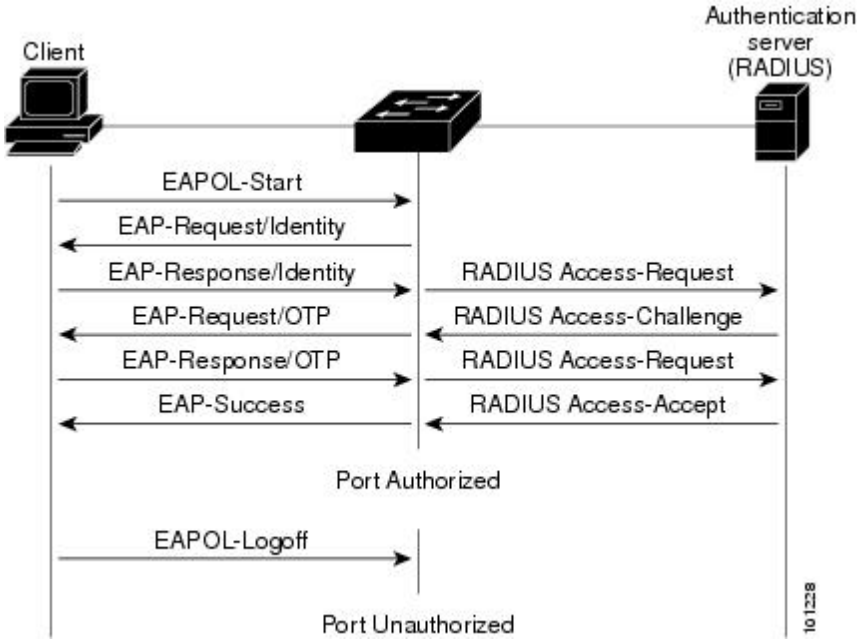
Note If 802.1x authentication is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client sends frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized. If the authentication fails, authentication can be retried, the port might be assigned to a VLAN that provides limited services, or network access is not granted.

The specific exchange of EAP frames depends on the authentication method being used.

Figure 59: Message Exchange

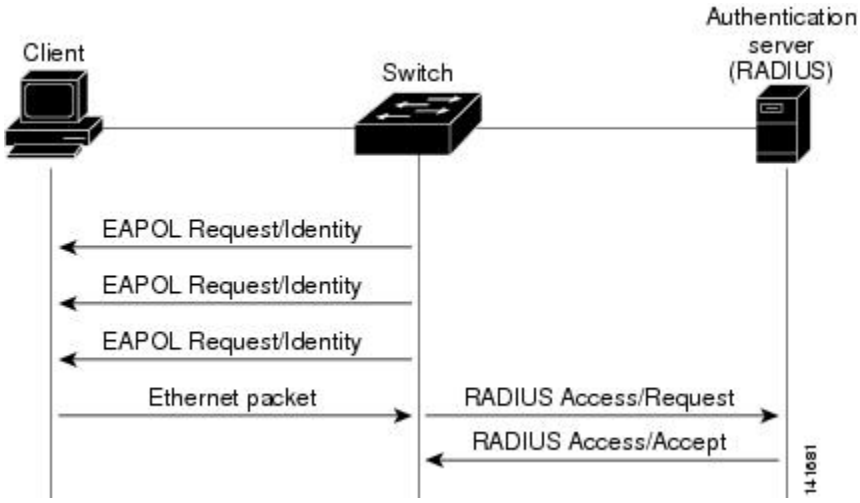
This figure shows a message exchange initiated by the client when the client uses the One-Time-Password (OTP) authentication method with a RADIUS server.



If 802.1x authentication times out while waiting for an EAPOL message exchange and MAC authentication bypass is enabled, the switch can authorize the client when the switch detects an Ethernet packet from the client. The switch uses the MAC address of the client as its identity and includes this information in the RADIUS-access/request frame that is sent to the RADIUS server. After the server sends the switch the RADIUS-access/accept frame (authorization is successful), the port becomes authorized. If authorization fails and a guest VLAN is specified, the switch assigns the port to the guest VLAN. If the switch detects an EAPOL packet while waiting for an Ethernet packet, the switch stops the MAC authentication bypass process and starts 802.1x authentication.

Figure 60: Message Exchange During MAC Authentication Bypass

This figure shows the message exchange during MAC authentication bypass.



Authentication Manager for Port-Based Authentication

Port-Based Authentication Methods

Table 71: 802.1x Features

Authentication method	Mode			
	Single host	Multiple host	MDA	Multiple Authentication
802.1x	VLAN assignment Per-user ACL Filter-ID attribute Downloadable ACL Redirect URL	VLAN assignment	VLAN assignment Per-user ACL Filter-Id attribute Downloadable ACL Redirect URL	VLAN assignment Per-user ACL Filter-Id attribute Downloadable ACL Redirect URL
MAC authentication bypass	VLAN assignment Per-user ACL Filter-ID attribute Downloadable ACL Redirect URL	VLAN assignment	VLAN assignment Per-user ACL Filter-Id attribute Downloadable ACL Redirect URL	VLAN assignment Per-user ACL Filter-Id attribute Downloadable ACL Redirect URL
Standalone web authentication	Proxy ACL, Filter-Id attribute, downloadable ACL			
NAC Layer 2 IP validation	Filter-Id attribute Downloadable ACL Redirect URL	Filter-Id attribute Downloadable ACL Redirect URL	Filter-Id attribute Downloadable ACL Redirect URL	Filter-Id attribute Downloadable ACL Redirect URL
Web authentication as fallback method	Proxy ACL Filter-Id attribute Downloadable ACL	Proxy ACL Filter-Id attribute Downloadable ACL	Proxy ACL Filter-Id attribute Downloadable ACL	Proxy ACL Filter-Id attribute Downloadable ACL

[14] Supported in Cisco IOS Release 12.2(50)SE and later.
[15] For clients that do not support 802.1x authentication.

Per-User ACLs and Filter-Ids

Note You can only set **any** as the source in the ACL.

Note For any ACL configured for multiple-host mode, the source portion of statement must be *any*. (For example, **permit icmp** *any* **host 10.10.1.1**.)

You must specify **any** in the source ports of any defined ACL. Otherwise, the ACL cannot be applied and authorization fails. Single host is the only exception to support backward compatibility.

More than one host can be authenticated on MDA-enabled and multiauth ports. The ACL policy applied for one host does not effect the traffic of another host. If only one host is authenticated on a multi-host port, and the other hosts gain network access without authentication, the ACL policy for the first host can be applied to the other connected hosts by specifying any in the source address.

Port-Based Authentication Manager CLI Commands

The authentication-manager interface-configuration commands control all the authentication methods, such as 802.1x, MAC authentication bypass, and web authentication. The authentication manager commands determine the priority and order of authentication methods applied to a connected host.

The authentication manager commands control generic authentication features, such as host-mode, violation mode, and the authentication timer. Generic authentication commands include the **authentication host-mode**, **authentication violation**, and **authentication timer** interface configuration commands.

802.1x-specific commands begin with the **dot1x** keyword. For example, the **authentication port-control auto** interface configuration command enables authentication on an interface.

To disable dot1x on a switch, remove the configuration globally by using the no dot1x system-auth-control , and also remove it from all configured interfaces.

Note If 802.1x authentication is globally disabled, other authentication methods are still enabled on that port, such as web authentication.

The **authentication manager** commands provide the same functionality as earlier 802.1x commands.

When filtering out verbose system messages generated by the authentication manager, the filtered content typically relates to authentication success. You can also filter verbose messages for 802.1x authentication and MAB authentication. There is a separate command for each authentication method:

- The **no authentication logging verbose** global configuration command filters verbose messages from the authentication manager.
- The **no dot1x logging verbose** global configuration command filters 802.1x authentication verbose messages.
- The **no mab logging verbose** global configuration command filters MAC authentication bypass (MAB) verbose messages

Table 72: Authentication Manager Commands and Earlier 802.1x Commands

The authentication manager commands in Cisco IOS Release 12.2(50)SE or later	The equivalent 802.1x commands in Cisco IOS Release 12.2(46)SE and earlier	Description
authentication control-direction {**both** | **in**}	**dot1x control-direction** {**both** | **in**}	Enable 802.1x authentication with the wake-on-LAN (WoL) feature, and configure the port control as unidirectional or bidirectional.
authentication event	**dot1x auth-fail vlan** **dot1x critical (interface configuration)** **dot1x guest-vlan6**	Enable the restricted VLAN on a port. Enable the inaccessible-authentication-bypass feature. Specify an active VLAN as an 802.1x guest VLAN.
authentication fallback *fallback-profile*	**dot1x fallback** *fallback-profile*	Configure a port to use web authentication as a fallback method for clients that do not support 802.1x authentication.
authentication host-mode [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]	**dot1x host-mode** {**single-host** | **multi-host** | **multi-domain**}	Allow a single host (client) or multiple hosts on an 802.1x-authorized port.
authentication order	**mab**	Provides the flexibility to define the order of authentication methods to be used.
authentication periodic	**dot1x reauthentication**	Enable periodic re-authentication of the client.
authentication port-control {**auto** | **force-authorized** | **force-un authorized**}	**dot1x port-control** {**auto** | **force-authorized** | **force-unauthorized**}	Enable manual control of the authorization state of the port.
authentication timer	**dot1x timeout**	Set the 802.1x timers.
authentication violation {**protect** | **restrict** | **shutdown**}	**dot1x violation-mode** {**shutdown** | **restrict** | **protect**}	Configure the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.

Ports in Authorized and Unauthorized States

During 802.1x authentication, depending on the switch port state, the switch can grant a client access to the network. The port starts in the *unauthorized* state. While in this state, the port that is not configured as a voice VLAN port disallows all ingress and egress traffic except for 802.1x authentication, CDP, and STP packets. When a client is successfully authenticated, the port changes to the *authorized* state, allowing all traffic for the client to flow normally. If the port is configured as a voice VLAN port, the port allows VoIP traffic and 802.1x protocol packets before the client is successfully authenticated.

Note CDP bypass is not supported and may cause a port to go into err-disabled state.

If a client that does not support 802.1x authentication connects to an unauthorized 802.1x port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1x-enabled client connects to a port that is not running the 802.1x standard, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state.

You control the port authorization state by using the **authentication port-control** interface configuration command and these keywords:

- **force-authorized**—disables 802.1x authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without 802.1x-based authentication of the client. This is the default setting.
- **force-unauthorized**—causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port.
- **auto**—enables 802.1x authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the switch by using the client MAC address.

If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can resend the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message, causing the switch port to change to the unauthorized state.

If the link state of a port changes from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

Port-Based Authentication and Switch Stacks

If a switch is added to or removed from a switch stack, 802.1x authentication is not affected as long as the IP connectivity between the RADIUS server and the stack remains intact. This statement also applies if the stack master is removed from the switch stack. Note that if the stack master fails, a stack member becomes the new stack master by using the election process, and the 802.1x authentication process continues as usual.

If IP connectivity to the RADIUS server is interrupted because the switch that was connected to the server is removed or fails, these events occur:

- Ports that are already authenticated and that do not have periodic re-authentication enabled remain in the authenticated state. Communication with the RADIUS server is not required.
- Ports that are already authenticated and that have periodic re-authentication enabled (with the **dot1x re-authentication** global configuration command) fail the authentication process when the re-authentication occurs. Ports return to the unauthenticated state during the re-authentication process. Communication with the RADIUS server is required.

  For an ongoing authentication, the authentication fails immediately because there is no server connectivity.

If the switch that failed comes up and rejoins the switch stack, the authentications might or might not fail depending on the boot-up time and whether the connectivity to the RADIUS server is re-established by the time the authentication is attempted.

To avoid loss of connectivity to the RADIUS server, you should ensure that there is a redundant connection to it. For example, you can have a redundant connection to the stack master and another to a stack member, and if the stack master fails, the switch stack still has connectivity to the RADIUS server.

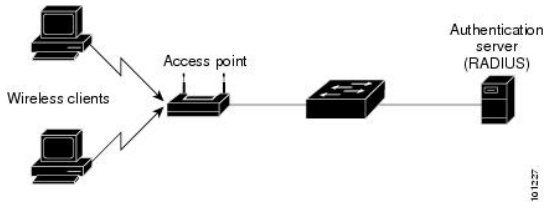
802.1x Host Mode

You can configure an 802.1x port for single-host or for multiple-hosts mode. In single-host mode, only one client can be connected to the 802.1x-enabled switch port. The switch detects the client by sending an EAPOL frame when the port link state changes to the up state. If a client leaves or is replaced with another client, the switch changes the port link state to down, and the port returns to the unauthorized state.

In multiple-hosts mode, you can attach multiple hosts to a single 802.1x-enabled port. In this mode, only one of the attached clients must be authorized for all clients to be granted network access. If the port becomes unauthorized (re-authentication fails or an EAPOL-logoff message is received), the switch denies network access to all of the attached clients.

In this topology, the wireless access point is responsible for authenticating the clients attached to it, and it also acts as a client to the switch.

Figure 61: Multiple Host Mode Example



Note For all host modes, the line protocol stays up before authorization when port-based authentication is configured.

The switch supports multidomain authentication (MDA), which allows both a data device and a voice device, such as an IP Phone (Cisco or non-Cisco), to connect to the same switch port.

802.1x Multiple Authentication Mode

Multiple-authentication (multiauth) mode allows multiple authenticated clients on the data VLAN. Each host is individually authenticated. If a voice VLAN is configured, this mode also allows one client on the VLAN. (If the port detects any additional voice clients, they are discarded from the port, but no violation errors occur.)

If a hub or access point is connected to an 802.1x-enabled port, each connected client must be authenticated. For non-802.1x devices, you can use MAC authentication bypass or web authentication as the per-host authentication fallback method to authenticate different hosts with different methods on a single port.

There is no limit to the number of data hosts can authenticate on a multiauthport. However, only one voice device is allowed if the voice VLAN is configured. Since there is no host limit defined violation will not be trigger, if a second voice is seen we silently discard it but do not trigger violation. For MDA functionality on the voice VLAN, multiple-authentication mode assigns authenticated devices to either a data or a voice VLAN, depending on the VSAs received from the authentication server.

Note When a port is in multiple-authentication mode, the guest VLAN and the authentication-failed VLAN features do not activate.

You can assign a RADIUS-server-supplied VLAN in multi-auth mode, under the following conditions:

- The host is the first host authorized on the port, and the RADIUS server supplies VLAN information
- Subsequent hosts are authorized with a VLAN that matches the operational VLAN.
- A host is authorized on the port with no VLAN assignment, and subsequent hosts either have no VLAN assignment, or their VLAN information matches the operational VLAN.
- The first host authorized on the port has a group VLAN assignment, and subsequent hosts either have no VLAN assignment, or their group VLAN matches the group VLAN on the port. Subsequent hosts must use the same VLAN from the VLAN group as the first host. If a VLAN list is used, all hosts are subject to the conditions specified in the VLAN list.
- Only one voice VLAN assignment is supported on a multi-auth port.
- After a VLAN is assigned to a host on the port, subsequent hosts must have matching VLAN information or be denied access to the port.
- You cannot configure a guest VLAN or an auth-fail VLAN in multi-auth mode.
- The behavior of the critical-auth VLAN is not changed for multi-auth mode. When a host tries to authenticate and the server is not reachable, all authorized hosts are reinitialized in the configured VLAN.

Multi-auth Per User VLAN assignment

The Multi-auth Per User VLAN assignment feature allows you to create multiple operational access VLANs based on VLANs assigned to the clients on the port that has a single configured access VLAN. The port configured as an access port where the traffic for all the VLANs associated with data domain is not dot1q tagged, and these VLANs are treated as native VLANs.

The number of hosts per multi-auth port is 8, however there can be more hosts.

Note The Multi-auth Per User VLAN assignment feature is not supported for Voice domain. All clients in Voice domain on a port must use the same VLAN.

The following scenarios are associated with the multi-auth Per User VLAN assignments:

Scenario one

When a hub is connected to an access port, and the port is configured with an access VLAN (V0).

The host (H1) is assigned to VLAN (V1) through the hub. The operational VLAN of the port is changed to V1. This behaviour is similar on a single-host or multi-domain-auth port.

When a second host (H2) is connected and gets assigned to VLAN (V2), the port will have two operational VLANs (V1 and V2). If H1 and H2 sends untagged ingress traffic, H1 traffic is mapped to VLAN (V1) and H2 traffic to VLAN (V2), all egress traffic going out of the port on VLAN (V1) and VLAN (V2) are untagged.

If both the hosts, H1 and H2 are logged out or the sessions are removed due to some reason then VLAN (V1) and VLAN (V2) are removed from the port, and the configured VLAN (V0) is restored on the port.

Scenario two

When a hub is connected to an access port, and the port is configured with an access VLAN (V0). The host (H1) is assigned to VLAN (V1) through the hub. The operational VLAN of the port is changed to V1.

When a second host (H2) is connected and gets authorized without explicit vlan policy, H2 is expected to use the configured VLAN (V0) that is restored on the port. A ll egress traffic going out of two operational VLANs, VLAN (V0) and VLAN (V1) are untagged.

If host (H2) is logged out or the session is removed due to some reason then the configured VLAN (V0) is removed from the port, and VLAN (V1) becomes the only operational VLAN on the port.

Scenario three

When a hub is connected to an access port in open mode, and the port is configured with an access VLAN (V0) .

The host (H1) is assigned to VLAN (V1) through the hub. The operational VLAN of the port is changed to V1. When a second host (H2) is connected and remains unauthorized, it still has access to operational VLAN (V1) due to open mode.

If host H1 is logged out or the session is removed due to some reason, VLAN (V1) is removed from the port and host (H2) gets assigned to VLAN (V0).

Note The combination of Open mode and VLAN assignment has an adverse affect on host (H2) because it has an IP address in the subnet that corresponds to VLAN (V1).

Limitation in Multi-auth Per User VLAN assignment

In the Multi-auth Per User VLAN assignment feature, egress traffic from multiple vlans are untagged on a port where the hosts receive traffic that is not meant for them. This can be a problem with broadcast and multicast traffic.

- **IPv4 ARPs**: Hosts receive ARP packets from other subnets. This is a problem if two subnets in different Virtual Routing and Forwarding (VRF) tables with overlapping IP address range are active on the port. The host ARP cache may get invalid entries.
- I**Pv6 control packets**: In IPv6 deployments, Router Advertisements (RA) are processed by hosts that are not supposed to receive them. When a host from one VLAN receives RA from a different VLAN, the host assign incorrect IPv6 address to itself. Such a host is unable to get access to the network.

  The workaround is to enable the IPv6 first hop security so that the broadcast ICMPv6 packets are converted to unicast and sent out from multi-auth enabled ports.. The packet is replicated for each client in multi-auth port belonging to the VLAN and the destination MAC is set to an individual client. Ports having one VLAN, ICMPv6 packets broadcast normally.
- **IP multicast**: Multicast traffic destined to a multicast group gets replicated for different VLANs if the hosts on those VLANs join the multicast group. When two hosts in different VLANs join a multicast group (on the same mutli-auth port), two copies of each multicast packet are sent out from that port.

MAC Move

When a MAC address is authenticated on one switch port, that address is not allowed on another authentication manager-enabled port of the switch. If the switch detects that same MAC address on another authentication manager-enabled port, the address is not allowed.

There are situations where a MAC address might need to move from one port to another on the same switch. For example, when there is another device (for example a hub or an IP phone) between an authenticated host and a switch port, you might want to disconnect the host from the device and connect it directly to another port on the same switch.

You can globally enable MAC move so the device is reauthenticated on the new port. When a host moves to a second port, the session on the first port is deleted, and the host is reauthenticated on the new port. MAC move is supported on all host modes. (The authenticated host can move to any port on the switch, no matter which host mode is enabled on the that port.) When a MAC address moves from one port to another, the switch terminates the authenticated session on the original port and initiates a new authentication sequence on the new port. The MAC move feature applies to both voice and data hosts.

Note In open authentication mode, a MAC address is immediately moved from the original port to the new port, with no requirement for authorization on the new port.

MAC Replace

The MAC replace feature can be configured to address the violation that occurs when a host attempts to connect to a port where another host was previously authenticated.

Note This feature does not apply to ports in multi-auth mode, because violations are not triggered in that mode. It does not apply to ports in multiple host mode, because in that mode, only the first host requires authentication.

If you configure the **authentication violation** interface configuration command with the **replace** keyword, the authentication process on a port in multi-domain mode is:

- A new MAC address is received on a port with an existing authenticated MAC address.
- The authentication manager replaces the MAC address of the current data host on the port with the new MAC address.
- The authentication manager initiates the authentication process for the new MAC address.
- If the authentication manager determines that the new host is a voice host, the original voice host is removed.

If a port is in open authentication mode, any new MAC address is immediately added to the MAC address table.

802.1x Accounting

The 802.1x standard defines how users are authorized and authenticated for network access but does not keep track of network usage. 802.1x accounting is disabled by default. You can enable 802.1x accounting to monitor this activity on 802.1x-enabled ports:

- User successfully authenticates.
- User logs off.
- Link-down occurs.
- Re-authentication successfully occurs.
- Re-authentication fails.

The switch does not log 802.1x accounting information. Instead, it sends this information to the RADIUS server, which must be configured to log accounting messages.

802.1x Accounting Attribute-Value Pairs

The information sent to the RADIUS server is represented in the form of Attribute-Value (AV) pairs. These AV pairs provide data for different applications. (For example, a billing application might require information that is in the Acct-Input-Octets or the Acct-Output-Octets attributes of a RADIUS packet.)

AV pairs are automatically sent by a switch that is configured for 802.1x accounting. Three types of RADIUS accounting packets are sent by a switch:

- START–sent when a new user session starts
- INTERIM–sent during an existing session for updates
- STOP–sent when a session terminates

You can view the AV pairs that are being sent by the switch by entering the **debug radius accounting** privileged EXEC command. For more information about this command, see the *Cisco IOS Debug Command Reference, Release 12.4.*

This table lists the AV pairs and when they are sent are sent by the switch.

Table 73: Accounting AV Pairs

Attribute Number	AV Pair Name	START	INTERIM	STOP
Attribute[1]	User-Name	Always	Always	Always
Attribute[4]	NAS-IP-Address	Always	Always	Always
Attribute[5]	NAS-Port	Always	Always	Always
Attribute[8]	Framed-IP-Address	Never	Sometimes[16]	Sometimes
Attribute[25]	Class	Always	Always	Always
Attribute[30]	Called-Station-ID	Always	Always	Always
Attribute[31]	Calling-Station-ID	Always	Always	Always
Attribute[40]	Acct-Status-Type	Always	Always	Always
Attribute[41]	Acct-Delay-Time	Always	Always	Always
Attribute[42]	Acct-Input-Octets	Never	Always	Always
Attribute[43]	Acct-Output-Octets	Never	Always	Always
Attribute[47]	Acct-Input-Packets	Never	Always	Always
Attribute[48]	Acct-Output-Packets	Never	Always	Always
Attribute[44]	Acct-Session-ID	Always	Always	Always
Attribute[45]	Acct-Authentic	Always	Always	Always
Attribute[46]	Acct-Session-Time	Never	Always	Always
Attribute[49]	Acct-Terminate-Cause	Never	Never	Always
Attribute[61]	NAS-Port-Type	Always	Always	Always

[16] The Framed-IP-Address AV pair is sent when a valid static IP address is configured or w when a Dynamic Host Control Protocol (DHCP) binding exists for the host in the DHCP snooping bindings table.

802.1x Readiness Check

The 802.1x readiness check monitors 802.1x activity on all the switch ports and displays information about the devices connected to the ports that support 802.1x. You can use this feature to determine if the devices connected to the switch ports are 802.1x-capable. You use an alternate authentication such as MAC authentication bypass or web authentication for the devices that do not support 802.1x functionality.

This feature only works if the supplicant on the client supports a query with the NOTIFY EAP notification packet. The client must respond within the 802.1x timeout value.

Switch-to-RADIUS-Server Communication

RADIUS security servers are identified by their hostname or IP address, hostname and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authentication—the second host entry configured acts as the fail-over backup to the first one. The RADIUS host entries are tried in the order that they were configured.

802.1x Authentication with VLAN Assignment

The switch supports 802.1x authentication with VLAN assignment. After successful 802.1x authentication of a port, the RADIUS server sends the VLAN assignment to configure the switch port. The RADIUS server database maintains the username-to-VLAN mappings, assigning the VLAN based on the username of the client connected to the switch port. You can use this feature to limit network access for certain users.

Voice device authentication is supported with multidomain host mode in Cisco IOS Release 12.2(37)SE. In Cisco IOS Release 12.2(40)SE and later, when a voice device is authorized and the RADIUS server returned an authorized VLAN, the voice VLAN on the port is configured to send and receive packets on the assigned voice VLAN. Voice VLAN assignment behaves the same as data VLAN assignment on multidomain authentication (MDA)-enabled ports.

When configured on the switch and the RADIUS server, 802.1x authentication with VLAN assignment has these characteristics:

- If no VLAN is supplied by the RADIUS server or if 802.1x authentication is disabled, the port is configured in its access VLAN after successful authentication. Recall that an access VLAN is a VLAN assigned to an access port. All packets sent from or received on this port belong to this VLAN.
- If 802.1x authentication is enabled but the VLAN information from the RADIUS server is not valid, authorization fails and configured VLAN remains in use. This prevents ports from appearing unexpectedly in an inappropriate VLAN because of a configuration error.

  Configuration errors could include specifying a VLAN for a routed port, a malformed VLAN ID, a nonexistent or internal (routed port) VLAN ID, an RSPAN VLAN, a shut down or suspended VLAN. In the case of a multidomain host port, configuration errors can also be due to an attempted assignment of a data VLAN that matches the configured or assigned voice VLAN ID (or the reverse).
- If 802.1x authentication is enabled and all information from the RADIUS server is valid, the authorized device is placed in the specified VLAN after authentication.
- If the multiple-hosts mode is enabled on an 802.1x port, all hosts are placed in the same VLAN (specified by the RADIUS server) as the first authenticated host.
- Enabling port security does not impact the RADIUS server-assigned VLAN behavior.
- If 802.1x authentication is disabled on the port, it is returned to the configured access VLAN and configured voice VLAN.

- If an 802.1x port is authenticated and put in the RADIUS server-assigned VLAN, any change to the port access VLAN configuration does not take effect. In the case of a multidomain host, the same applies to voice devices when the port is fully authorized with these exceptions:
  - If the VLAN configuration change of one device results in matching the other device configured or assigned VLAN, then authorization of all devices on the port is terminated and multidomain host mode is disabled until a valid configuration is restored where data and voice device configured VLANs no longer match.
  - If a voice device is authorized and is using a downloaded voice VLAN, the removal of the voice VLAN configuration, or modifying the configuration value to dot1p or untagged results in voice device un-authorization and the disablement of multi-domain host mode.

When the port is in the force authorized, force unauthorized, unauthorized, or shutdown state, it is put into the configured access VLAN.

If an 802.1x port is authenticated and put in the RADIUS server-assigned VLAN, any change to the port access VLAN configuration does not take effect. In the case of a multidomain host, the same applies to voice devices when the port is fully authorized with these exceptions:

- If the VLAN configuration change of one device results in matching the other device configured or assigned VLAN, authorization of all devices on the port is terminated and multidomain host mode is disabled until a valid configuration is restored where data and voice device configured VLANs no longer match.
- If a voice device is authorized and is using a downloaded voice VLAN, the removal of the voice VLAN configuration, or modifying the configuration value to *dot1p* or *untagged* results in voice device un-authorization and the disablement of multi-domain host mode.

When the port is in the force authorized, force unauthorized, unauthorized, or shutdown state, it is put into the configured access VLAN.

The 802.1x authentication with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN Membership Policy Server (VMPS).

To configure VLAN assignment you need to perform these tasks:

- Enable AAA authorization by using the **network** keyword to allow interface configuration from the RADIUS server.
- Enable 802.1x authentication. (The VLAN assignment feature is automatically enabled when you configure 802.1x authentication on an access port).
- Assign vendor-specific tunnel attributes in the RADIUS server. The RADIUS server must return these attributes to the switch:
  - [64] Tunnel-Type = VLAN
  - [65] Tunnel-Medium-Type = 802
  - [81] Tunnel-Private-Group-ID = VLAN name or VLAN ID
  - [83] Tunnel-Preference

  Attribute [64] must contain the value *VLAN* (type 13). Attribute [65] must contain the value *802* (type 6). Attribute [81] specifies the *VLAN name* or *VLAN ID* assigned to the IEEE 802.1x-authenticated user.

802.1x Authentication with Per-User ACLs

You can enable per-user access control lists (ACLs) to provide different levels of network access and service to an 802.1x-authenticated user. When the RADIUS server authenticates a user connected to an 802.1x port, it retrieves the ACL attributes based on the user identity and sends them to the switch. The switch applies the attributes to the 802.1x port for the duration of the user session. The switch removes the per-user ACL configuration when the session is over, if authentication fails, or if a link-down condition occurs. The switch does not save RADIUS-specified ACLs in the running configuration. When the port is unauthorized, the switch removes the ACL from the port.

You can configure router ACLs and input port ACLs on the same switch. However, a port ACL takes precedence over a router ACL. If you apply input port ACL to an interface that belongs to a VLAN, the port ACL takes precedence over an input router ACL applied to the VLAN interface. Incoming packets received on the port to which a port ACL is applied are filtered by the port ACL. Incoming routed packets received on other ports are filtered by the router ACL. Outgoing routed packets are filtered by the router ACL. To avoid configuration conflicts, you should carefully plan the user profiles stored on the RADIUS server.

RADIUS supports per-user attributes, including vendor-specific attributes. These vendor-specific attributes (VSAs) are in octet-string format and are passed to the switch during the authentication process. The VSAs used for per-user ACLs are inacl#<*n*> for the ingress direction and outacl#<*n*> for the egress direction. MAC ACLs are supported only in the ingress direction. The switch supports VSAs only in the ingress direction. It does not support port ACLs in the egress direction on Layer 2 ports.

Use only the extended ACL syntax style to define the per-user configuration stored on the RADIUS server. When the definitions are passed from the RADIUS server, they are created by using the extended naming convention. However, if you use the Filter-Id attribute, it can point to a standard ACL.

You can use the Filter-Id attribute to specify an inbound or outbound ACL that is already configured on the switch. The attribute contains the ACL number followed by *.in* for ingress filtering or *.out* for egress filtering. If the RADIUS server does not allow the *.in* or *.out* syntax, the access list is applied to the outbound ACL by default. Because of limited support of Cisco IOS access lists on the switch, the Filter-Id attribute is supported only for IP ACLs numbered 1 to 199 and 1300 to 2699 (IP standard and IP extended ACLs).

The maximum size of the per-user ACL is 4000 ASCII characters but is limited by the maximum size of RADIUS-server per-user ACLs.

To configure per-user ACLs:

- Enable AAA authentication.
- Enable AAA authorization by using the **network** keyword to allow interface configuration from the RADIUS server.
- Enable 802.1x authentication.
- Configure the user profile and VSAs on the RADIUS server.
- Configure the 802.1x port for single-host mode.

Note Per-user ACLs are supported only in single-host mode.

802.1x Authentication with Downloadable ACLs and Redirect URLs

You can download ACLs and redirect URLs from a RADIUS server to the switch during 802.1x authentication or MAC authentication bypass of the host. You can also download ACLs during web authentication.

Note A downloadable ACL is also referred to as a *dACL.*

If more than one host is authenticated and the host is in single-host, MDA, or multiple-authentication mode, the switch changes the source address of the ACL to the host IP address.

You can apply the ACLs and redirect URLs to all the devices connected to the 802.1x-enabled port.

If no ACLs are downloaded during 802.1x authentication, the switch applies the static default ACL on the port to the host. On a voice VLAN port configured in multi-auth or MDA mode, the switch applies the ACL only to the phone as part of the authorization policies.

Note The limit for dACL with stacking is 64 ACEs per dACL per port. The limit without stacking is the number of available TCAM entries which varies based on the other ACL features that are active.

Beginning with Cisco IOS Release 12.2(55)SE, if there is no static ACL on a port, a dynamic auth-default ACL is created, and policies are enforced before dACLs are downloaded and applied.

Note The auth-default-ACL does not appear in the running configuration.

The auth-default ACL is created when at least one host with an authorization policy is detected on the port. The auth-default ACL is removed from the port when the last authenticated session ends. You can configure the auth-default ACL by using the **ip access-list extended auth-default-acl** global configuration command.

Note The auth-default-ACL does not support Cisco Discovery Protocol (CDP) bypass in the single host mode. You must configure a static ACL on the interface to support CDP bypass.

The 802.1x and MAB authentication methods support two authentication modes, *open* and *closed*. If there is no static ACL on a port in *closed* authentication mode:

- An auth-default-ACL is created.
- The auth-default-ACL allows only DHCP traffic until policies are enforced.
- When the first host authenticates, the authorization policy is applied without IP address insertion.
- When a second host is detected, the policies for the first host are refreshed, and policies for the first and subsequent sessions are enforced with IP address insertion.

If there is no static ACL on a port in *open* authentication mode:

- An auth-default-ACL-OPEN is created and allows all traffic.

- Policies are enforced with IP address insertion to prevent security breaches.
- Web authentication is subject to the auth-default-ACL-OPEN.

To control access for hosts with no authorization policy, you can configure a directive. The supported values for the directive are *open* and *default*. When you configure the *open* directive, all traffic is allowed. The *default* directive subjects traffic to the access provided by the port. You can configure the directive either in the user profile on the AAA server or on the switch. To configure the directive on the AAA server, use the **authz-directive =<open/default>** global command. To configure the directive on the switch, use the **epm access-control open** global configuration command.

Note The default value of the directive is *default*.

If a host falls back to web authentication on a port without a configured ACL:

- If the port is in open authentication mode, the auth-default-ACL-OPEN is created.
- If the port is in closed authentication mode, the auth-default-ACL is created.

The access control entries (ACEs) in the fallback ACL are converted to per-user entries. If the configured fallback profile does not include a fallback ACL, the host is subject to the auth-default-ACL associated with the port.

Note If you use a custom logo with web authentication and it is stored on an external server, the port ACL must allow access to the external server before authentication. You must either configure a static port ACL or change the auth-default-ACL to provide appropriate access to the external server.

Cisco Secure ACS and Attribute-Value Pairs for the Redirect URL

The switch uses these *cisco-av-pair* VSAs:

- url-redirect is the HTTP or HTTPS URL.
- url-redirect-acl is the switch ACL name or number.

The switch uses the CiscoSecure-defined-ACL attribute value pair to intercept an HTTP or HTTPS request from the end point. The switch then forwards the client web browser to the specified redirect address. The url-redirect AV pair on the Cisco Secure ACS contains the URL to which the web browser is redirected. The url-redirect-acl attribute value pair contains the name or number of an ACL that specifies the HTTP or HTTPS traffic to redirect.

Note

- Traffic that matches a permit ACE in the ACL is redirected.
- An ACE that matches permit rule of the url-redirect-acl gets the client redirected to url-redirect page. The client traffic is allowed when a deny rule is matched.
- Define the URL redirect ACL and the default port ACL on the switch.

If a redirect URL is configured for a client on the authentication server, a default port ACL on the connected client switch port must also be configured.

When security ACL/dACL and punt/redirect ACLs are applied together to the session, the url-redirect-acl has the higher priority.

For more information about using redirect ACLs, refer the document here.

Cisco Secure ACS and Attribute-Value Pairs for Downloadable ACLs

You can set the CiscoSecure-Defined-ACL Attribute-Value (AV) pair on the Cisco Secure ACS with the RADIUS cisco-av-pair vendor-specific attributes (VSAs). This pair specifies the names of the downloadable ACLs on the Cisco Secure ACS with the #ACL#-IP-name-number attribute.

- The *name* is the ACL name.
- The *number* is the version number (for example, 3f783768).

If a downloadable ACL is configured for a client on the authentication server, a default port ACL on the connected client switch port must also be configured.

If the default ACL is configured on the switch and the Cisco Secure ACS sends a host-access-policy to the switch, it applies the policy to traffic from the host connected to a switch port. If the policy does not apply, the switch applies the default ACL. If the Cisco Secure ACS sends the switch a downloadable ACL, this ACL takes precedence over the default ACL that is configured on the switch port. However, if the switch receives an host access policy from the Cisco Secure ACS but the default ACL is not configured, the authorization failure is declared.

VLAN ID-based MAC Authentication

You can use VLAN ID-based MAC authentication if you wish to authenticate hosts based on a static VLAN ID instead of a downloadable VLAN. When you have a static VLAN policy configured on your switch, VLAN information is sent to an IAS (Microsoft) RADIUS server along with the MAC address of each host for authentication. The VLAN ID configured on the connected port is used for MAC authentication. By using VLAN ID-based MAC authentication with an IAS server, you can have a fixed number of VLANs in the network.

The feature also limits the number of VLANs monitored and handled by STP. The network can be managed as a fixed VLAN.

Note This feature is not supported on Cisco ACS Server. (The ACS server ignores the sent VLAN-IDs for new hosts and only authenticates based on the MAC address.)

802.1x Authentication with Guest VLAN

You can configure a guest VLAN for each 802.1x port on the switch to provide limited services to clients, such as downloading the 802.1x client. These clients might be upgrading their system for 802.1x authentication, and some hosts, such as Windows 98 systems, might not be IEEE 802.1x-capable.

When you enable a guest VLAN on an 802.1x port, the switch assigns clients to a guest VLAN when the switch does not receive a response to its EAP request/identity frame or when EAPOL packets are not sent by the client.

The switch maintains the EAPOL packet history. If an EAPOL packet is detected on the interface during the lifetime of the link, the switch determines that the device connected to that interface is an IEEE 802.1x-capable supplicant, and the interface does not change to the guest VLAN state. EAPOL history is cleared if the interface link status goes down. If no EAPOL packet is detected on the interface, the interface changes to the guest VLAN state.

If the switch is trying to authorize an 802.1x-capable voice device and the AAA server is unavailable, the authorization attempt fails, but the detection of the EAPOL packet is saved in the EAPOL history. When the AAA server becomes available, the switch authorizes the voice device. However, the switch no longer allows other devices access to the guest VLAN. To prevent this situation, use one of these command sequences:

- Enter the **authentication event no-response action authorize vlan** *vlan-id* interface configuration command to allow access to the guest VLAN.
- Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command to restart the port.

If devices send EAPOL packets to the switch during the lifetime of the link, the switch no longer allows clients that fail authentication access to the guest VLAN.

Note If an EAPOL packet is detected after the interface has changed to the guest VLAN, the interface reverts to an unauthorized state, and 802.1x authentication restarts.

Any number of 802.1x-incapable clients are allowed access when the switch port is moved to the guest VLAN. If an 802.1x-capable client joins the same port on which the guest VLAN is configured, the port is put into the unauthorized state in the user-configured access VLAN, and authentication is restarted.

Guest VLANs are supported on 802.1x ports in single host, multiple host, multi-auth and multi-domain modes.

You can configure any active VLAN except an RSPAN VLAN, a private VLAN, or a voice VLAN as an 802.1x guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

The switch supports *MAC authentication bypass*. When MAC authentication bypass is enabled on an 802.1x port, the switch can authorize clients based on the client MAC address when IEEE 802.1x authentication times out while waiting for an EAPOL message exchange. After detecting a client on an 802.1x port, the switch waits for an Ethernet packet from the client. The switch sends the authentication server a RADIUS-access/request frame with a username and password based on the MAC address. If authorization succeeds, the switch grants the client access to the network. If authorization fails, the switch assigns the port to the guest VLAN if one is specified.

802.1x Authentication with Restricted VLAN

You can configure a restricted VLAN (also referred to as an *authentication failed VLAN*) for each IEEE 802.1x port on a switch stack or a switch to provide limited services to clients that cannot access the guest VLAN. These clients are 802.1x-compliant and cannot access another VLAN because they fail the authentication process. A restricted VLAN allows users without valid credentials in an authentication server (typically,

visitors to an enterprise) to access a limited set of services. The administrator can control the services available to the restricted VLAN.

Note You can configure a VLAN to be both the guest VLAN and the restricted VLAN if you want to provide the same services to both types of users.

Without this feature, the client attempts and fails authentication indefinitely, and the switch port remains in the spanning-tree blocking state. With this feature, you can configure the switch port to be in the restricted VLAN after a specified number of authentication attempts (the default value is 3 attempts).

The authenticator counts the failed authentication attempts for the client. When this count exceeds the configured maximum number of authentication attempts, the port moves to the restricted VLAN. The failed attempt count increments when the RADIUS server replies with either an *EAP failure* or an empty response without an EAP packet. When the port moves into the restricted VLAN, the failed attempt counter resets.

Users who fail authentication remain in the restricted VLAN until the next re-authentication attempt. A port in the restricted VLAN tries to re-authenticate at configured intervals (the default is 60 seconds). If re-authentication fails, the port remains in the restricted VLAN. If re-authentication is successful, the port moves either to the configured VLAN or to a VLAN sent by the RADIUS server. You can disable re-authentication. If you do this, the only way to restart the authentication process is for the port to receive a *link down* or *EAP logoff* event. We recommend that you keep re-authentication enabled if a client might connect through a hub. When a client disconnects from the hub, the port might not receive the *link down* or *EAP logoff* event.

After a port moves to the restricted VLAN, a simulated EAP success message is sent to the client. This prevents clients from indefinitely attempting authentication. Some clients (for example, devices running Windows XP) cannot implement DHCP without EAP success.

Restricted VLANs are supported on 802.1x ports in all host modes and on Layer 2 ports.

You can configure any active VLAN except an RSPAN VLAN, a primary private VLAN, or a voice VLAN as an 802.1x restricted VLAN. The restricted VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

Other security port features such as dynamic ARP Inspection, DHCP snooping, and IP source guard can be configured independently on a restricted VLAN.

802.1x Authentication with Inaccessible Authentication Bypass

Use the inaccessible authentication bypass feature, also referred to as *critical authentication* or the *AAA fail policy*, when the switch cannot reach the configured RADIUS servers and new hosts cannot be authenticated. You can configure the switch to connect those hosts to *critical ports.*

When a new host tries to connect to the critical port, that host is moved to a user-specified access VLAN, the *critical VLAN*. The administrator gives limited authentication to the hosts.

When the switch tries to authenticate a host connected to a critical port, the switch checks the status of the configured RADIUS server. If a server is available, the switch can authenticate the host. However, if all the RADIUS servers are unavailable, the switch grants network access to the host and puts the port in the *critical-authentication* state, which is a special case of the authentication state.

Note If *critical authentication* is configured on interface, then vlan used for critical authorization (*critical vlan*) should be active on the switch. If the *critical vlan* is inactive (or) down, *critical authentication* session will keep trying to enable inactive vlan and fail repeatedly. This can lead to large amount of memory holding.

Inaccessible Authentication Bypass Support on Multiple-Authentication Ports

When a port is configured on any host mode and the AAA server is unavailable, the port is then configured to multi-host mode and moved to the critical VLAN. To support this inaccessible bypass on multiple-authentication (multiauth) ports, use the **authentication event server dead action reinitialize vlan** *vlan-id* command. When a new host tries to connect to the critical port, that port is reinitialized and all the connected hosts are moved to the user-specified access VLAN.

This command is supported on all host modes.

Inaccessible Authentication Bypass Authentication Results

The behavior of the inaccessible authentication bypass feature depends on the authorization state of the port:

- If the port is unauthorized when a host connected to a critical port tries to authenticate and all servers are unavailable, the switch puts the port in the critical-authentication state in the RADIUS-configured or user-specified access VLAN.
- If the port is already authorized and reauthentication occurs, the switch puts the critical port in the critical-authentication state in the current VLAN, which might be the one previously assigned by the RADIUS server.
- If the RADIUS server becomes unavailable during an authentication exchange, the current exchange times out, and the switch puts the critical port in the critical-authentication state during the next authentication attempt.

You can configure the critical port to reinitialize hosts and move them out of the critical VLAN when the RADIUS server is again available. When this is configured, all critical ports in the critical-authentication state are automatically re-authenticated.

Inaccessible Authentication Bypass Feature Interactions

Inaccessible authentication bypass interacts with these features:

- Guest VLAN—Inaccessible authentication bypass is compatible with guest VLAN. When a guest VLAN is enabled on 8021.x port, the features interact as follows:
  - If at least one RADIUS server is available, the switch assigns a client to a guest VLAN when the switch does not receive a response to its EAP request/identity frame or when EAPOL packets are not sent by the client.
  - If all the RADIUS servers are not available and the client is connected to a critical port, the switch authenticates the client and puts the critical port in the critical-authentication state in the RADIUS-configured or user-specified access VLAN.
  - If all the RADIUS servers are not available and the client is not connected to a critical port, the switch might not assign clients to the guest VLAN if one is configured.

- If all the RADIUS servers are not available and if a client is connected to a critical port and was previously assigned to a guest VLAN, the switch keeps the port in the guest VLAN.

- Restricted VLAN—If the port is already authorized in a restricted VLAN and the RADIUS servers are unavailable, the switch puts the critical port in the critical-authentication state in the restricted VLAN.
- 802.1x accounting—Accounting is not affected if the RADIUS servers are unavailable.
- Private VLAN—You can configure inaccessible authentication bypass on a private VLAN host port. The access VLAN must be a secondary private VLAN.
- Voice VLAN—Inaccessible authentication bypass is compatible with voice VLAN, but the RADIUS-configured or user-specified access VLAN and the voice VLAN must be different.
- Remote Switched Port Analyzer (RSPAN)—Do not configure an RSPAN VLAN as the RADIUS-configured or user-specified access VLAN for inaccessible authentication bypass.

In a switch stack:

- The stack master checks the status of the RADIUS servers by sending keepalive packets. When the status of a RADIUS server changes, the stack master sends the information to the stack members. The stack members can then check the status of RADIUS servers when re-authenticating critical ports.
- If the new stack master is elected, the link between the switch stack and RADIUS server might change, and the new stack immediately sends keepalive packets to update the status of the RADIUS servers. If the server status changes from *dead* to *alive*, the switch re-authenticates all switch ports in the critical-authentication state.

When a member is added to the stack, the stack master sends the member the server status.

Note Switch stacks are supported only on Catalyst 2960-S switches running the LAN base image.

802.1x Critical Voice VLAN

When an IP phone connected to a port is authenticated by the access control server (ACS), the phone is put into the voice domain. If the ACS is not reachable, the switch cannot determine if the device is a voice device. If the server is unavailable, the phone cannot access the voice network and therefore cannot operate.

For data traffic, you can configure inaccessible authentication bypass, or critical authentication, to allow traffic to pass through on the native VLAN when the server is not available. If the RADIUS authentication server is unavailable (down) and inaccessible authentication bypass is enabled, the switch grants the client access to the network and puts the port in the critical-authentication state in the RADIUS-configured or the user-specified access VLAN. When the switch cannot reach the configured RADIUS servers and new hosts cannot be authenticated, the switch connects those hosts to critical ports. A new host trying to connect to the critical port is moved to a user-specified access VLAN, the critical VLAN, and granted limited authentication.

You can enter the **authentication event server dead action authorize voice** interface configuration command to configure the critical voice VLAN feature. When the ACS does not respond, the port goes into critical authentication mode. When traffic coming from the host is tagged with the voice VLAN, the connected device (the phone) is put in the configured voice VLAN for the port. The IP phones learn the voice VLAN identification through CDP (Cisco devices) or through LLDP or DHCP.

You can configure the voice VLAN for a port by entering the **switchport voice vlan** *vlan-id* interface configuration command.

This feature is supported in multidomain and multi-auth host modes. Although you can enter the command when the switch in single-host or multi-host mode, the command has no effect unless the device changes to multidomain or multi-auth host mode.

802.1x User Distribution

You can configure 802.1x user distribution to load-balance users with the same group name across multiple different VLANs.

The VLANs are either supplied by the RADIUS server or configured through the switch CLI under a VLAN group name.

- Configure the RADIUS server to send more than one VLAN name for a user. The multiple VLAN names can be sent as part of the response to the user. The 802.1x user distribution tracks all the users in a particular VLAN and achieves load balancing by moving the authorized user to the least populated VLAN.
- Configure the RADIUS server to send a VLAN group name for a user. The VLAN group name can be sent as part of the response to the user. You can search for the selected VLAN group name among the VLAN group names that you configured by using the switch CLI. If the VLAN group name is found, the corresponding VLANs under this VLAN group name are searched to find the least populated VLAN. Load balancing is achieved by moving the corresponding authorized user to that VLAN.

Note The RADIUS server can send the VLAN information in any combination of VLAN-IDs, VLAN names, or VLAN groups.

802.1x User Distribution Configuration Guidelines

- Confirm that at least one VLAN is mapped to the VLAN group.
- You can map more than one VLAN to a VLAN group.
- You can modify the VLAN group by adding or deleting a VLAN.
- When you clear an existing VLAN from the VLAN group name, none of the authenticated ports in the VLAN are cleared, but the mappings are removed from the existing VLAN group.
- If you clear the last VLAN from the VLAN group name, the VLAN group is cleared.
- You can clear a VLAN group even when the active VLANs are mapped to the group. When you clear a VLAN group, none of the ports or users that are in the authenticated state in any VLAN within the group are cleared, but the VLAN mappings to the VLAN group are cleared.

IEEE 802.1x Authentication with Voice VLAN Ports

A voice VLAN port is a special access port associated with two VLAN identifiers:

- VVID to carry voice traffic to and from the IP phone. The VVID is used to configure the IP phone connected to the port.
- PVID to carry the data traffic to and from the workstation connected to the switch through the IP phone. The PVID is the native VLAN of the port.

The IP phone uses the VVID for its voice traffic, regardless of the authorization state of the port. This allows the phone to work independently of IEEE 802.1x authentication.

In single-host mode, only the IP phone is allowed on the voice VLAN. In multiple-hosts mode, additional clients can send traffic on the voice VLAN after a supplicant is authenticated on the PVID. When multiple-hosts mode is enabled, the supplicant authentication affects both the PVID and the VVID.

A voice VLAN port becomes active when there is a link, and the device MAC address appears after the first CDP message from the IP phone. Cisco IP phones do not relay CDP messages from other devices. As a result, if several IP phones are connected in series, the switch recognizes only the one directly connected to it. When IEEE 802.1x authentication is enabled on a voice VLAN port, the switch drops packets from unrecognized IP phones more than one hop away.

When IEEE 802.1x authentication is enabled on a switch port, you can configure an access port VLAN that is also a voice VLAN.

When IP phones are connected to an 802.1x-enabled switch port that is in single host mode, the switch grants the phones network access without authenticating them. We recommend that you use multidomain authentication (MDA) on the port to authenticate both a data device and a voice device, such as an IP phone

Note If you enable IEEE 802.1x authentication on an access port on which a voice VLAN is configured and to which a Cisco IP Phone is connected, the Cisco IP phone loses connectivity to the switch for up to 30 seconds.

IEEE 802.1x Authentication with Port Security

In general, Cisco does not recommend enabling port security when IEEE 802.1x is enabled. Since IEEE 802.1x enforces a single MAC address per port (or per VLAN when MDA is configured for IP telephony), port security is redundant and in some cases may interfere with expected IEEE 802.1x operations.

IEEE 802.1x Authentication with Wake-on-LAN

The IEEE 802.1x authentication with wake-on-LAN (WoL) feature allows dormant PCs to be powered when the switch receives a specific Ethernet frame, known as the *magic packet*. You can use this feature in environments where administrators need to connect to systems that have been powered down.

When a host that uses WoL is attached through an IEEE 802.1x port and the host powers off, the IEEE 802.1x port becomes unauthorized. The port can only receive and send EAPOL packets, and WoL magic packets cannot reach the host. When the PC is powered off, it is not authorized, and the switch port is not opened.

When the switch uses IEEE 802.1x authentication with WoL, the switch forwards traffic to unauthorized IEEE 802.1x ports, including magic packets. While the port is unauthorized, the switch continues to block ingress traffic other than EAPOL packets. The host can receive packets but cannot send packets to other devices in the network.

Note If PortFast is not enabled on the port, the port is forced to the bidirectional state.

When you configure a port as unidirectional by using the **authentication control-direction in** interface configuration command, the port changes to the spanning-tree forwarding state. The port can send packets to the host but cannot receive packets from the host.

When you configure a port as bidirectional by using the **authentication control-direction both** interface configuration command, the port is access-controlled in both directions. The port does not receive packets from or send packets to the host.

IEEE 802.1x Authentication with MAC Authentication Bypass

You can configure the switch to authorize clients based on the client MAC address by using the MAC authentication bypass feature. For example, you can enable this feature on IEEE 802.1x ports connected to devices such as printers.

If IEEE 802.1x authentication times out while waiting for an EAPOL response from the client, the switch tries to authorize the client by using MAC authentication bypass.

When the MAC authentication bypass feature is enabled on an IEEE 802.1x port, the switch uses the MAC address as the client identity. The authentication server has a database of client MAC addresses that are allowed network access. After detecting a client on an IEEE 802.1x port, the switch waits for an Ethernet packet from the client. The switch sends the authentication server a RADIUS-access/request frame with a username and password based on the MAC address. If authorization succeeds, the switch grants the client access to the network. If authorization fails, the switch assigns the port to the guest VLAN if one is configured. This process works for most client devices; however, it does not work for clients that use an alternate MAC address format. You can configure how MAB authentication is performed for clients with MAC addresses that deviate from the standard format or where the RADIUS configuration requires the user name and password to differ.

If an EAPOL packet is detected on the interface during the lifetime of the link, the switch determines that the device connected to that interface is an 802.1x-capable supplicant and uses 802.1x authentication (not MAC authentication bypass) to authorize the interface. EAPOL history is cleared if the interface link status goes down.

If the switch already authorized a port by using MAC authentication bypass and detects an IEEE 802.1x supplicant, the switch does not unauthorize the client connected to the port. When re-authentication occurs, the switch uses the authentication or re-authentication methods configured on the port, if the previous session ended because the Termination-Action RADIUS attribute value is DEFAULT.

Clients that were authorized with MAC authentication bypass can be re-authenticated. The re-authentication process is the same as that for clients that were authenticated with IEEE 802.1x. During re-authentication, the port remains in the previously assigned VLAN. If re-authentication is successful, the switch keeps the port in the same VLAN. If re-authentication fails, the switch assigns the port to the guest VLAN, if one is configured.

If re-authentication is based on the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute [29]) and if the Termination-Action RADIUS attribute (Attribute [29]) action is *Initialize* (the attribute value is *DEFAULT*), the MAC authentication bypass session ends, and connectivity is lost during re-authentication. If MAC authentication bypass is enabled and the IEEE 802.1x authentication times out, the switch uses the MAC authentication bypass feature to initiate re-authorization. For more information about these AV pairs, see RFC 3580, “IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines.”

MAC authentication bypass interacts with the features:

- IEEE 802.1x authentication—You can enable MAC authentication bypass only if 802.1x authentication is enabled on the port .
- Guest VLAN—If a client has an invalid MAC address identity, the switch assigns the client to a guest VLAN if one is configured.
- Restricted VLAN—This feature is not supported when the client connected to an IEEE 802.lx port is authenticated with MAC authentication bypass.
- Port security
- Voice VLAN
- Private VLAN—You can assign a client to a private VLAN.
- Network Edge Access Topology (NEAT)—MAB and NEAT are mutually exclusive. You cannot enable MAB when NEAT is enabled on an interface, and you should not enable NEAT when MAB is enabled on an interface.

Cisco IOS Release 12.2(55)SE and later supports filtering of verbose MAB system messages

Network Admission Control Layer 2 IEEE 802.1x Validation

The switch supports the Network Admission Control (NAC) Layer 2 IEEE 802.1x validation, which checks the antivirus condition or *posture* of endpoint systems or clients before granting the devices network access. With NAC Layer 2 IEEE 802.1x validation, you can do these tasks:

- Download the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute[29]) from the authentication server.
- Set the number of seconds between re-authentication attempts as the value of the Session-Timeout RADIUS attribute (Attribute[27]) and get an access policy against the client from the RADIUS server.
- Set the action to be taken when the switch tries to re-authenticate the client by using the Termination-Action RADIUS attribute (Attribute[29]). If the value is the *DEFAULT* or is not set, the session ends. If the value is RADIUS-Request, the re-authentication process starts.
- Set the list of VLAN number or name or VLAN group name as the value of the Tunnel Group Private ID (Attribute[81]) and the preference for the VLAN number or name or VLAN group name as the value of the Tunnel Preference (Attribute[83]). If you do not configure the Tunnel Preference, the first Tunnel Group Private ID (Attribute[81]) attribute is picked up from the list.
- View the NAC posture token, which shows the posture of the client, by using the **show authentication** privileged EXEC command.
- Configure secondary private VLANs as guest VLANs.

Configuring NAC Layer 2 IEEE 802.1x validation is similar to configuring IEEE 802.1x port-based authentication except that you must configure a posture token on the RADIUS server.

Flexible Authentication Ordering

You can use flexible authentication ordering to configure the order of methods that a port uses to authenticate a new host. The IEEE 802.1X Flexible Authentication feature supports three authentication methods:

- dot1X—IEEE 802.1X authentication is a Layer 2 authentication method.
- mab—MAC-Authentication Bypass is a Layer 2 authentication method.
- webauth—Web authentication is a Layer 3 authentication method.

Using this feature, you can control which ports use which authentication methods, and you can control the failover sequencing of methods on those ports. For example, MAC authentication bypass and 802.1x can be the primary or secondary authentication methods, and web authentication can be the fallback method if either or both of those authentication attempts fail.

The IEEE 802.1X Flexible Authentication feature supports the following host modes:

- multi-auth—Multiauthentication allows one authentication on a voice VLAN and multiple authentications on the data VLAN.
- multi-domain—Multidomain authentication allows two authentications: one on the voice VLAN and one on the data VLAN.

Open1x Authentication

Open1x authentication allows a device access to a port before that device is authenticated. When open authentication is configured, a new host can pass traffic according to the access control list (ACL) defined on the port. After the host is authenticated, the policies configured on the RADIUS server are applied to that host.

You can configure open authentication with these scenarios:

- Single-host mode with open authentication–Only one user is allowed network access before and after authentication.
- MDA mode with open authentication–Only one user in the voice domain and one user in the data domain are allowed.
- Multiple-hosts mode with open authentication–Any host can access the network.
- Multiple-authentication mode with open authentication–Similar to MDA, except multiple hosts can be authenticated.

Note If open authentication is configured, it takes precedence over other authentication controls. This means that if you use the **authentication open** interface configuration command, the port will grant access to the host irrespective of the **authentication port-control** interface configuration command.

Multidomain Authentication

The switch supports multidomain authentication (MDA), which allows both a data device and voice device, such as an IP phone (Cisco or non-Cisco), to authenticate on the same switch port. The port is divided into a data domain and a voice domain.

Note For all host modes, the line protocol stays up before authorization when port-based authentication is configured.

MDA does not enforce the order of device authentication. However, for best results, we recommend that a voice device is authenticated before a data device on an MDA-enabled port.

Follow these guidelines for configuring MDA:

- You must configure a switch port for MDA.
- You must configure the voice VLAN for the IP phone when the host mode is set to multidomain.
- Voice VLAN assignment on an MDA-enabled port is supported Cisco IOS Release 12.2(40)SE and later.
- To authorize a voice device, the AAA server must be configured to send a Cisco Attribute-Value (AV) pair attribute with a value of *device-traffic-class=voice*. Without this value, the switch treats the voice device as a data device.
- The guest VLAN and restricted VLAN features only apply to the data devices on an MDA-enabled port. The switch treats a voice device that fails authorization as a data device.
- If more than one device attempts authorization on either the voice or the data domain of a port, it is error disabled.
- Until a device is authorized, the port drops its traffic. Non-Cisco IP phones or voice devices are allowed into both the data and voice VLANs. The data VLAN allows the voice device to contact a DHCP server to obtain an IP address and acquire the voice VLAN information. After the voice device starts sending on the voice VLAN, its access to the data VLAN is blocked.
- A voice device MAC address that is binding on the data VLAN is not counted towards the port security MAC address limit.
- MDA can use MAC authentication bypass as a fallback mechanism to allow the switch port to connect to devices that do not support IEEE 802.1x authentication.
- When a *data* or a *voice* device is detected on a port, its MAC address is blocked until authorization succeeds. If the authorization fails, the MAC address remains blocked for 5 minutes.
- If more than five devices are detected on the *data* VLAN or more than one voice device is detected on the *voice* VLAN while a port is unauthorized, the port is error disabled.
- When a port host mode is changed from single- or multihost to multidomain mode, an authorized data device remains authorized on the port. However, a Cisco IP phone that has been allowed on the port voice VLAN is automatically removed and must be reauthenticated on that port.
- Active fallback mechanisms such as guest VLAN and restricted VLAN remain configured after a port changes from single- or multihost mode to multidomain mode.
- Switching a port host mode from multidomain to single- or multihost mode removes all authorized devices from the port.

- If a data domain is authorized first and placed in the guest VLAN, non-IEEE 802.1x-capable voice devices need to tag their packets on the voice VLAN to trigger authentication.
- We do not recommend per-user ACLs with an MDA-enabled port. An authorized device with a per-user ACL policy might impact traffic on both the voice and data VLANs of the port. If used, only one device on the port should enforce per-user ACLs.

Limiting Login for Users

The Limiting Login feature helps Network administrators to limit the login attempt of users to a network. When a user fails to successfully login to a network within a configurable number of attempts within a configurable time limit, the user can be blocked. This feature is enabled only for local users and not for remote users. You need to configure the **aaa authentication rejected** command in global configuration mode to enable this feature.

802.1x Supplicant and Authenticator Switches with Network Edge Access Topology (NEAT)

The Network Edge Access Topology (NEAT) feature extends identity to areas outside the wiring closet (such as conference rooms). This allows any type of device to authenticate on the port.

- 802.1x switch supplicant: You can configure a switch to act as a supplicant to another switch by using the 802.1x supplicant feature. This configuration is helpful in a scenario, where, for example, a switch is outside a wiring closet and is connected to an upstream switch through a trunk port. A switch configured with the 802.1x switch supplicant feature authenticates with the upstream switch for secure connectivity. Once the supplicant switch authenticates successfully the port mode changes from access to trunk in an authenticator switch. In a supplicant switch you must manually configure trunk when enabling CISP.
- If the access VLAN is configured on the authenticator switch, it becomes the native VLAN for the trunk port after successful authentication.

In the default state, when you connect a supplicant switch to an authenticator switch that has BPDU guard enabled, the authenticator port could be error-disabled if it receives a Spanning Tree Protocol (STP) bridge protocol data unit (BPDU) packets before the supplicant switch has authenticated. Beginning with Cisco IOS Release 15.0(1)SE, you can control traffic exiting the supplicant port during the authentication period. Entering the **dot1x supplicant controlled transient** global configuration command temporarily blocks the supplicant port during authentication to ensure that the authenticator port does not shut down before authentication completes. If authentication fails, the supplicant port opens. Entering the **no dot1x supplicant controlled transient** global configuration command opens the supplicant port during the authentication period. This is the default behavior.

We strongly recommend using the **dot1x supplicant controlled transient**command on a supplicant switch when BPDU guard is enabled on the authenticator switch port with the **spanning-tree bpduguard enable** interface configuration command.

Note If you globally enable BPDU guard on the authenticator switch by using the **spanning-tree portfast bpduguard default** global configuration command, entering the **dot1x supplicant controlled transient** command does not prevent the BPDU violation.

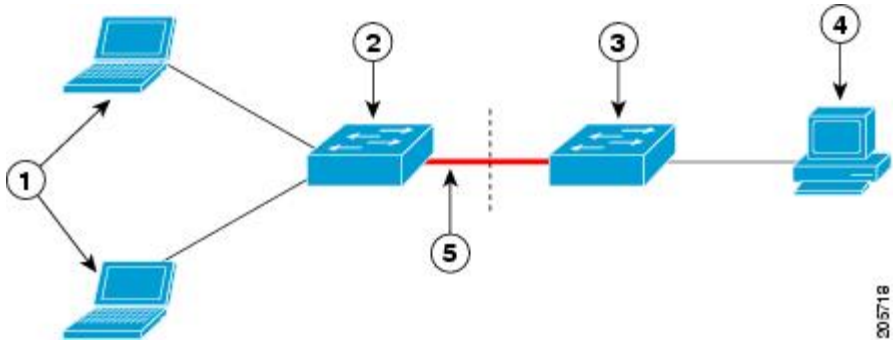
You can enable MDA or multiauth mode on the authenticator switch interface that connects to one more supplicant switches. Multihost mode is not supported on the authenticator switch interface.

When you reboot an authenticator switch with single-host mode enabled on the interface, the interface may move to err-disabled state before authentication. To recover from err-disabled state, flap the authenticator port to activate the interface again and initiate authentication.

Use the **dot1x supplicant force-multicast** global configuration command on the supplicant switch for Network Edge Access Topology (NEAT) to work in all host modes.

- Host Authorization: Ensures that only traffic from authorized hosts (connecting to the switch with supplicant) is allowed on the network. The switches use Client Information Signalling Protocol (CISP) to send the MAC addresses connecting to the supplicant switch to the authenticator switch.
- Auto enablement: Automatically enables trunk configuration on the authenticator switch, allowing user traffic from multiple VLANs coming from supplicant switches. Configure the cisco-av-pair as *device-traffic-class=switch* at the ACS. (You can configure this under the *group* or the *user* settings.)

Figure 62: Authenticator and Supplicant Switch using CISP



1	Workstations (clients)	2	Supplicant switch (outside wiring closet)
3	Authenticator switch	4	Access control server (ACS)
5	Trunk port		

Note The **switchport nonegotiate** command is not supported on supplicant and authenticator switches with NEAT. This command should not be configured at the supplicant side of the topology. If configured on the authenticator side, the internal macros will automatically remove this command from the port.

Voice Aware 802.1x Security

Note To use voice aware IEEE 802.1x authentication, the switch must be running the LAN base image.

You use the voice aware 802.1x security feature to configure the switch to disable only the VLAN on which a security violation occurs, whether it is a data or voice VLAN. In previous releases, when an attempt to authenticate the data client caused a security violation, the entire port shut down, resulting in a complete loss of connectivity.

You can use this feature in IP phone deployments where a PC is connected to the IP phone. A security violation found on the data VLAN results in the shutdown of only the data VLAN. The traffic on the voice VLAN flows through the switch without interruption.

Common Session ID

Authentication manager uses a single session ID (referred to as a common session ID) for a client no matter which authentication method is used. This ID is used for all reporting purposes, such as the show commands and MIBs. The session ID appears with all per-session syslog messages.

The session ID includes:

- The IP address of the Network Access Device (NAD)
- A monotonically increasing unique 32 bit integer
- The session start time stamp (a 32 bit integer)

This example shows how the session ID appears in the output of the show authentication command. The session ID in this example is 160000050000000B288508E5:

```
Switch# show authentication sessions
Interface  MAC Address     Method   Domain   Status         Session ID
Fa4/0/4    0000.0000.0203  mab      DATA     Authz Success  160000050000000B288508E5
```

This is an example of how the session ID appears in the syslog output. The session ID in this example is also160000050000000B288508E5:

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

The session ID is used by the NAD, the AAA server, and other report-analyzing applications to identify the client. The ID appears automatically. No configuration is required.

How to Configure 802.1x Port-Based Authentication

Default 802.1x Authentication Configuration

Table 74: Default 802.1x Authentication Configuration

Feature	Default Setting
Switch 802.1x enable state	Disabled.
Per-port 802.1x enable state	Disabled (force-authorized). The port sends and receives normal traffic without 802.1x-based authentication of the client.
AAA	Disabled.
RADIUS server • IP address • UDP authentication port • Default accounting port • Key	• None specified. • 1645. • 1646. • None specified.
Host mode	Single-host mode.
Control direction	Bidirectional control.
Periodic re-authentication	Disabled.
Number of seconds between re-authentication attempts	3600 seconds.
Re-authentication number	2 times (number of times that the switch restarts the authentication process before the port changes to the unauthorized state).
Quiet period	60 seconds (number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client).
Retransmission time	30 seconds (number of seconds that the switch should wait for a response to an EAP request/identity frame from the client before resending the request).
Maximum retransmission number	2 times (number of times that the switch will send an EAP-request/identity frame before restarting the authentication process).

Feature	Default Setting
Client timeout period	30 seconds (when relaying a request from the authentication server to the client, the amount of time the switch waits for a response before resending the request to the client.)
Authentication server timeout period	30 seconds (when relaying a response from the client to the authentication server, the amount of time the switch waits for a reply before resending the response to the server.) You can change this timeout period by using the dot1x timeout server-timeout interface configuration command.
Inactivity timeout	Disabled.
Guest VLAN	None specified.
Inaccessible authentication bypass	Disabled.
Restricted VLAN	None specified.
Authenticator (switch) mode	None specified.
MAC authentication bypass	Disabled.
Voice-aware security	Disabled.

802.1x Authentication Configuration Guidelines

802.1x Authentication

These are the 802.1x authentication configuration guidelines:

- When 802.1x authentication is enabled, ports are authenticated before any other Layer 2 or Layer 3 features are enabled.
- If the VLAN to which an 802.1x-enabled port is assigned changes, this change is transparent and does not affect the switch. For example, this change occurs if a port is assigned to a RADIUS server-assigned VLAN and is then assigned to a different VLAN after re-authentication.

  If the VLAN to which an 802.1x port is assigned to shut down, disabled, or removed, the port becomes unauthorized. For example, the port is unauthorized after the access VLAN to which a port is assigned shuts down or is removed.
- The 802.1x protocol is supported on Layer 2 static-access ports, voice VLAN ports, and Layer 3 routed ports, but it is not supported on these port types:
  - Dynamic ports—A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1x authentication on a dynamic port, an error message appears, and 802.1x authentication is not enabled. If you try to change the mode of an 802.1x-enabled port to dynamic, an error message appears, and the port mode is not changed.

- EtherChannel port—Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an 802.1x port. If you try to enable 802.1x authentication on an EtherChannel port, an error message appears, and 802.1x authentication is not enabled.
- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports—You can enable 802.1x authentication on a port that is a SPAN or RSPAN destination port. However, 802.1x authentication is disabled until the port is removed as a SPAN or RSPAN destination port. You can enable 802.1x authentication on a SPAN or RSPAN source port.

- Before globally enabling 802.1x authentication on a switch by entering the **dot1x system-auth-control** global configuration command, remove the EtherChannel configuration from the interfaces on which 802.1x authentication and EtherChannel are configured.
- Cisco IOS Release 12.2(55)SE and later supports filtering of system messages related to 802.1x authentication.

VLAN Assignment, Guest VLAN, Restricted VLAN, and Inaccessible Authentication Bypass

These are the configuration guidelines for VLAN assignment, guest VLAN, restricted VLAN, and inaccessible authentication bypass:

- When 802.1x authentication is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.
- The 802.1x authentication with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VMPS.
- You can configure any VLAN except an RSPAN VLAN or a voice VLAN as an 802.1x guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.
- After you configure a guest VLAN for an 802.1x port to which a DHCP client is connected, you might need to get a host IP address from a DHCP server. You can change the settings for restarting the 802.1x authentication process on the switch before the DHCP process on the client times out and tries to get a host IP address from the DHCP server. Decrease the settings for the 802.1x authentication process (**authentication timer inactivity** and **authentication timer reauthentication** interface configuration commands). The amount to decrease the settings depends on the connected 802.1x client type.
- When configuring the inaccessible authentication bypass feature, follow these guidelines:
  - The feature is supported on 802.1x port in single-host mode and multihosts mode.
  - If the client is running Windows XP and the port to which the client is connected is in the critical-authentication state, Windows XP might report that the interface is not authenticated.
  - If the Windows XP client is configured for DHCP and has an IP address from the DHCP server, receiving an EAP-Success message on a critical port might not re-initiate the DHCP configuration process.
  - You can configure the inaccessible authentication bypass feature and the restricted VLAN on an 802.1x port. If the switch tries to re-authenticate a critical port in a restricted VLAN and all the RADIUS servers are unavailable, switch changes the port state to the critical authentication state and remains in the restricted VLAN.

- If the CTS links are in Critical Authentication mode and the master reloads, the policy where SGT was configured on a device will not be available on the new master. This is because the internal bindings will not be synced to the standby switch in a 3750-X switch stack.

- You can configure any VLAN except an RSPAN VLAN or a voice VLAN as an 802.1x restricted VLAN. The restricted VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.
- When wireless guest clients obtains IP from foreign client VLAN instead of anchor client VLAN, you should use the **ip dhcp required** command under the WLAN configuration to force clients to issue a new DHCP request. This prevents the clients from getting an incorrect IP at anchor.
- If the wired guest clients fail to get IP address after a Cisco WLC (foreign) reload, perform a shut/no shut on the ports used by the clients to reconnect them.

MAC Authentication Bypass

These are the MAC authentication bypass configuration guidelines:

- Unless otherwise stated, the MAC authentication bypass guidelines are the same as the 802.1x authentication guidelines.
- If you disable MAC authentication bypass from a port after the port has been authorized with its MAC address, the port state is not affected.
- If the port is in the unauthorized state and the client MAC address is not the authentication-server database, the port remains in the unauthorized state. However, if the client MAC address is added to the database, the switch can use MAC authentication bypass to re-authorize the port.
- If the port is in the authorized state, the port remains in this state until re-authorization occurs.
- You can configure a timeout period for hosts that are connected by MAC authentication bypass but are inactive. The range is 1to 65535 seconds.

Maximum Number of Allowed Devices Per Port

This is the maximum number of devices allowed on an 802.1x-enabled port:

- In single-host mode, only one device is allowed on the access VLAN. If the port is also configured with a voice VLAN, an unlimited number of Cisco IP phones can send and receive traffic through the voice VLAN.
- In multidomain authentication (MDA) mode, one device is allowed for the access VLAN, and one IP phone is allowed for the voice VLAN.
- In multihost mode, only one 802.1x supplicant is allowed on the port, but an unlimited number of non-802.1x hosts are allowed on the access VLAN. An unlimited number of devices are allowed on the voice VLAN.

Configuring 802.1x Readiness Check

The 802.1x readiness check monitors 802.1x activity on all the switch ports and displays information about the devices connected to the ports that support 802.1x. You can use this feature to determine if the devices connected to the switch ports are 802.1x-capable.

The 802.1x readiness check is allowed on all ports that can be configured for 802.1x. The readiness check is not available on a port that is configured as **dot1x force-unauthorized**.

Follow these steps to enable the 802.1x readiness check on the switch:

Before you begin

Follow these guidelines to enable the readiness check on the switch:

- The readiness check is typically used before 802.1x is enabled on the switch.
- If you use the **dot1x test eapol-capable** privileged EXEC command without specifying an interface, all the ports on the switch stack are tested.
- When you configure the **dot1x test eapol-capable** command on an 802.1x-enabled port, and the link comes up, the port queries the connected client about its 802.1x capability. When the client responds with a notification packet, it is 802.1x-capable. A syslog message is generated if the client responds within the timeout period. If the client does not respond to the query, the client is not 802.1x-capable. No syslog message is generated
- When you configure the **dot1x test eapol-capable** command on an 802.1x-enabled port, and the link comes up, the port queries the connected client about its 802.1x capability. When the client responds with a notification packet, it is 802.1x-capable. A syslog message is generated if the client responds within the timeout period. If the client does not respond to the query, the client is not 802.1x-capable. No syslog message is generated
- The readiness check can be sent on a port that handles multiple hosts (for example, a PC that is connected to an IP phone). A syslog message is generated for each of the clients that respond to the readiness check within the timer period.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**dot1x test eapol-capable** [**interface** *interface-id*] **Example:**	Enables the 802.1x readiness check on the switch. (Optional) For *interface-id* specify the port on which to check for IEEE 802.1x readiness.

	Command or Action	Purpose
	`Switch# dot1x test eapol-capable interface gigabitethernet1/0/13` `DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL capable`	**Note** If you omit the optional **interface** keyword, all interfaces on the switch are tested.
Step 4	**dot1x test timeout** *timeout*	(Optional) Configures the timeout used to wait for EAPOL response. The range is from 1 to 65535 seconds. The default is 10 seconds.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Voice Aware 802.1x Security

Note To use voice aware IEEE 802.1x authentication, the switch must be running the LAN base image.

You use the voice aware 802.1x security feature on the switch to disable only the VLAN on which a security violation occurs, whether it is a data or voice VLAN. You can use this feature in IP phone deployments where a PC is connected to the IP phone. A security violation found on the data VLAN results in the shutdown of only the data VLAN. The traffic on the voice VLAN flows through the switch without interruption.

Follow these guidelines to configure voice aware 802.1x voice security on the switch:

- You enable voice aware 802.1x security by entering the **errdisable detect cause security-violation shutdown vlan** global configuration command. You disable voice aware 802.1x security by entering the **no** version of this command. This command applies to all 802.1x-configured ports in the switch.

  Note If you do not include the **shutdown vlan** keywords, the entire port is shut down when it enters the error-disabled state.

- If you use the **errdisable recovery cause security-violation** global configuration command to configure error-disabled recovery, the port is automatically re-enabled. If error-disabled recovery is not configured for the port, you re-enable it by using the **shutdown** and **no shutdown** interface configuration commands.
- You can re-enable individual VLANs by using the **clear errdisable interface** *interface-id* **vlan** [*vlan-list*] privileged EXEC command. If you do not specify a range, all VLANs on the port are enabled.

Beginning in privileged EXEC mode, follow these steps to enable voice aware 802.1x security:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**errdisable detect cause security-violation shutdown vlan**	Shut down any VLAN on which a security violation error occurs. **Note** If the **shutdown vlan** keywords are not included, the entire port enters the error-disabled state and shuts down.
Step 3	**errdisable recovery cause security-violation**	Enter global configuration mode.
Step 4	**clear errdisable interface***interface-id* **vlan** *[vlan-list]*	(Optional) Reenable individual VLANs that have been error disabled. • For interface-id specify the port on which to reenable individual VLANs. • (Optional) For vlan-list specify a list of VLANs to be re-enabled. If vlan-list is not specified, all VLANs are re-enabled.
Step 5	Enter the following: • **shutdown** • **no shutdown**	(Optional) Re-enable an error-disabled VLAN, and clear all error-disable indications.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show errdisable detect**	Verify your entries.

Example

This example shows how to configure the switch to shut down any VLAN on which a security violation error occurs:

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

This example shows how to re-enable all VLANs that were error disabled on port Gigabit Ethernet 40/2.

```
Switch# clear errdisable interface gigabitethernet4/0/2
vlan
```

You can verify your settings by entering the **show errdisable detect** privileged EXEC command.

Configuring 802.1x Violation Modes

You can configure an 802.1x port so that it shuts down, generates a syslog error, or discards packets from a new device when:

- a device connects to an 802.1x-enabled port
- the maximum number of allowed about devices have been authenticated on the port

Beginning in privileged EXEC mode, follow these steps to configure the security violation actions on the switch:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables AAA.
Step 3	**aaa authentication dot1x** {**default**} *method1* **Example:** `Switch(config)# aaa authentication dot1x default group radius`	Creates an 802.1x authentication method list. To create a default list that is used when a named list is *not* specified in the **authentication** command, use the **default** keyword followed by the method that is to be used in default situations. The default method list is automatically applied to all ports. For *method1*, enter the **group radius** keywords to use the list of all RADIUS servers for authentication.
Step 4	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/4`	Specifies the port connected to the client that is to be enabled for IEEE 802.1x authentication, and enter interface configuration mode.
Step 5	**switchport mode access** **Example:**	Sets the port to access mode.

	Command or Action	Purpose
	`Switch(config-if)# switchport mode access`	
Step 6	**authentication violation** {**shutdown** | **restrict** | **protect** | **replace**} **Example:** `Switch(config-if)# authentication violation restrict`	Configures the violation mode. The keywords have these meanings: • **shutdown**–Error disable the port. • **restrict**–Generate a syslog error. • **protect**–Drop packets from any new device that sends traffic to the port. • **replace**–Removes the current session and authenticates with the new host.
Step 7	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Configuring 802.1x Authentication

To allow per-user ACLs or VLAN assignment, you must enable AAA authorization to configure the switch for all network-related service requests.

This is the 802.1x AAA process:

Before you begin

To configure 802.1x port-based authentication, you must enable authentication, authorization, and accounting (AAA) and specify the authentication method list. A method list describes the sequence and authentication method to be queried to authenticate a user.

Procedure

	Command or Action	Purpose
Step 1	A user connects to a port on the switch.	
Step 2	Authentication is performed.	
Step 3	VLAN assignment is enabled, as appropriate, based on the RADIUS server configuration.	
Step 4	The switch sends a start message to an accounting server.	
Step 5	Re-authentication is performed, as necessary.	

	Command or Action	Purpose
Step 6	The switch sends an interim accounting update to the accounting server that is based on the result of re-authentication.	
Step 7	The user disconnects from the port.	
Step 8	The switch sends a stop message to the accounting server.	

Configuring 802.1x Port-Based Authentication

Beginning in privileged EXEC mode, follow these steps to configure 802.1x port-based authentication:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables AAA.
Step 3	**aaa authentication dot1x** {**default**} *method1* **Example:** `Switch(config)# aaa authentication dot1x default group radius`	Creates an 802.1x authentication method list. To create a default list that is used when a named list is *not* specified in the **authentication** command, use the **default** keyword followed by the method that is to be used in default situations. The default method list is automatically applied to all ports. For *method1*, enter the **group radius** keywords to use the list of all RADIUS servers for authentication. **Note** Though other keywords are visible in the command-line help string, only the **group radius** keywords are supported.
Step 4	**dot1x system-auth-control** **Example:**	Enables 802.1x authentication globally on the switch.

	Command or Action	Purpose
	`Switch(config)# dot1x system-auth-control`	
Step 5	**aaa authorization network** {**default**} **group radius** **Example:** `Switch(config)# aaa authorization network default group radius`	(Optional) Configures the switch to use user-RADIUS authorization for all network-related service requests, such as per-user ACLs or VLAN assignment.
Step 6	**radius server** *server name* **Example:** `Switch(config)# radius server rsim address ipv4 124.2.2.12`	(Optional) Specifies the IP address of the RADIUS server.
Step 7	**address** {**ipv4** | **ipv6**} *ip address* **Example:** `Switch(config-radius-server)# address ipv4 10.0.1.12`	Configures the IP address for the RADIUS server.
Step 8	**key** *string* **Example:** `Switch(config-radius-server)# key rad123`	(Optional) Specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.
Step 9	**exit** **Example:** `Switch(config-radius-server)# exit`	Exits the RADIUS server mode and enters the global configuration mode.
Step 10	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/2`	Specifies the port connected to the client that is to be enabled for IEEE 802.1x authentication, and enter interface configuration mode.
Step 11	**switchport mode access** **Example:** `Switch(config-if)# switchport mode`	(Optional) Sets the port to access mode only if you configured the RADIUS server in Step 6 and Step 7.

	Command or Action	Purpose
	`access`	
Step 12	**authentication port-control auto** **Example:** `Switch(config-if)# authentication port-control auto`	Enables 802.1x authentication on the port.
Step 13	**dot1x pae authenticator** **Example:** `Switch(config-if)# dot1x pae authenticator`	Sets the interface Port Access Entity to act only as an authenticator and ignore messages meant for a supplicant.
Step 14	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Configuring Switch-to-RADIUS-Server Communication

Follow these steps to configure the RADIUS server parameters:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip radius source-interface vlan** *vlan interface number* **Example:** `Switch(config)# ip radius`	Specifies that the RADIUS packets have the IP address of the indicated interface.

	Command or Action	Purpose
	`source-interface vlan 80`	
Step 4	**radius server** *server name* **Example:** `Switch(config)# radius server rsim address ipv4 124.2.2.12`	(Optional) Specifies the IP address of the RADIUS server.
Step 5	**address** {**ipv4** | **ipv6**} *ip address* **Example:** `Switch(config-radius-server)# address ipv4 10.0.1.2 auth-port 1550 acct-port 1560`	Configures the IP address for the RADIUS server.
Step 6	**key** *string* **Example:** `Switch(config-radius-server)# key rad123`	(Optional) Specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.
Step 7	**exit** **Example:** `Switch(config-radius-server)# exit`	Exits the RADIUS server mode and enters the global configuration mode.
Step 8	**radius-server dead-criteria tries** *num-tries* **Example:** `Switch(config)# radius-server dead-criteria tries 30`	Specifies the number of unanswered sent messages to a RADIUS server before considering the server to be inactive. The range of *num-tries* is 1 to 100.
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Configuring the Host Mode

Beginning in privileged EXEC mode, follow these steps to allow multiple hosts (clients) on an IEEE 802.1x-authorized port that has the **authentication port-control** interface configuration command set to **auto**. Use the **multi-domain** keyword to configure and enable multidomain authentication (MDA), which

allows both a host and a voice device, such as an IP phone (Cisco or non-Cisco), on the same switch port. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet2/0/1`	Specifies the port to which multiple hosts are indirectly attached, and enter interface configuration mode.
Step 3	**authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**] **Example:** `Switch(config-if)# authentication host-mode multi-host`	Allows multiple hosts (clients) on an 802.1x-authorized port. The keywords have these meanings: • **multi-auth**–Allow one client on the voice VLAN and multiple authenticated clients on the data VLAN. **Note** The **multi-auth** keyword is only available with the **authentication host-mode** command. • **multi-host**–Allow multiple hosts on an 802.1x-authorized port after a single host has been authenticated. • **multi-domain**–Allow both a host and a voice device, such as an IP phone (Cisco or non-Cisco), to be authenticated on an IEEE 802.1x-authorized port. **Note** You must configure the voice VLAN for the IP phone when the host mode is set to **multi-domain**. Make sure that the **authentication port-control** interface configuration command is set to **auto** for the specified interface.

	Command or Action	Purpose
Step 4	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Configuring Periodic Re-Authentication

You can enable periodic 802.1x client re-authentication and specify how often it occurs. If you do not specify a time period before enabling re-authentication, the number of seconds between attempts is 3600.

Beginning in privileged EXEC mode, follow these steps to enable periodic re-authentication of the client and to configure the number of seconds between re-authentication attempts. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet2/0/1`	Specifies the port to be configured, and enter interface configuration mode.
Step 3	**authentication periodic** **Example:** `Switch(config-if)# authentication periodic`	Enables periodic re-authentication of the client, which is disabled by default. **Note** The default value is 3600 seconds. To change the value of the reauthentication timer or to have the switch use a RADIUS-provided session timeout, enter the **authentication timer reauthenticate** command.
Step 4	**authentication timer** {{[**inactivity** | **reauthenticate** | **restart** | **unauthorized**]} {*value*}} **Example:** `Switch(config-if)# authentication timer`	Sets the number of seconds between re-authentication attempts. The **authentication timer** keywords have these meanings:

	Command or Action	Purpose
	`reauthenticate 180`	• **inactivity**—Interval in seconds after which if there is no activity from the client then it is unauthorized • **reauthenticate**—Time in seconds after which an automatic re-authentication attempt is initiated • **restart** *value*—Interval in seconds after which an attempt is made to authenticate an unauthorized port • **unauthorized** *value*—Interval in seconds after which an unauthorized session will get deleted This command affects the behavior of the switch only if periodic re-authentication is enabled.
Step 5	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Changing the Quiet Period

When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. The **authentication timer restart** interface configuration command controls the idle period. A failed authentication of the client might occur because the client provided an invalid password. You can provide a faster response time to the user by entering a number smaller than the default.

Beginning in privileged EXEC mode, follow these steps to change the quiet period. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface`	Specifies the port to be configured, and enter interface configuration mode.

	Command or Action	Purpose
	`gigabitethernet2/0/1`	
Step 3	**authentication timer restart** *seconds* **Example:** `Switch(config-if)# authentication timer restart 30`	Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 1 to 65535 seconds; the default is 60.
Step 4	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 5	**show authentication sessions interface** *interface-id* **Example:** `Switch# show authentication sessions interface gigabitethernet2/0/1`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Changing the Switch-to-Client Retransmission Time

The client responds to the EAP-request/identity frame from the switch with an EAP-response/identity frame. If the switch does not receive this response, it waits a set period of time (known as the retransmission time) and then resends the frame.

Note You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Beginning in privileged EXEC mode, follow these steps to change the amount of time that the switch waits for client notification. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet2/0/1`	Specifies the port to be configured, and enter interface configuration mode.
Step 3	**authentication timer reauthenticate** *seconds* **Example:** `Switch(config-if)# authentication timer reauthenticate 60`	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request. The range is 1 to 65535 seconds; the default is 5.
Step 4	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 5	**show authentication sessions interface** *interface-id* **Example:** `Switch# show authentication sessions interface gigabitethernet2/0/1`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Setting the Switch-to-Client Frame-Retransmission Number

In addition to changing the switch-to-client retransmission time, you can change the number of times that the switch sends an EAP-request/identity frame (assuming no response is received) to the client before restarting the authentication process.

Note You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Beginning in privileged EXEC mode, follow these steps to set the switch-to-client frame-retransmission number. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet2/0/1`	Specifies the port to be configured, and enter interface configuration mode.
Step 3	**dot1x max-reauth-req** *count* **Example:** `Switch(config-if)# dot1x max-reauth-req 5`	Sets the number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. The range is 1 to 10; the default is 2.
Step 4	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Setting the Re-Authentication Number

You can also change the number of times that the switch restarts the authentication process before the port changes to the unauthorized state.

Note You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Beginning in privileged EXEC mode, follow these steps to set the re-authentication number. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch# interface gigabitethernet2/0/1`	Specifies the port to be configured, and enter interface configuration mode.
Step 3	**switchport mode access** **Example:** `Switch(config-if)# switchport mode access`	Sets the port to access mode only if you previously configured the RADIUS server.
Step 4	**dot1x max-req** *count* **Example:** `Switch(config-if)# dot1x max-req 4`	Sets the number of times that the switch restarts the authentication process before the port changes to the unauthorized state. The range is 0 to 10; the default is 2.
Step 5	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Enabling MAC Move

MAC move allows an authenticated host to move from one port on the switch to another.

Beginning in privileged EXEC mode, follow these steps to globally enable MAC move on the switch. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**authentication mac-move permit** **Example:** `Switch(config)# authentication mac-move permit`	Enables MAC move on the switch. Default is deny. In Session Aware Networking mode, the default CLI is **access-session mac-move deny**. To enable Mac Move in Session Aware Networking, use the **no access-session mac-move** global configuration command. In legacy mode (IBNS 1.0), default value for **mac-move** is **deny** and in C3PL mode (IBNS 2.0) default value is **permit**.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 4	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 5	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Enabling MAC Replace

MAC replace allows a host to replace an authenticated host on a port.

Beginning in privileged EXEC mode, follow these steps to enable MAC replace on an interface. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet2/0/2`	Specifies the port to be configured, and enter interface configuration mode.
Step 3	**authentication violation** {**protect** | **replace** | **restrict** | **shutdown**} **Example:** `Switch(config-if)# authentication violation replace`	Use the **replace** keyword to enable MAC replace on the interface. The port removes the current session and initiates authentication with the new host. The other keywords have these effects: • **protect**: the port drops packets with unexpected MAC addresses without generating a system message. • **restrict**: violating packets are dropped by the CPU and a system message is generated. • **shutdown**: the port is error disabled when it receives an unexpected MAC address.
Step 4	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring 802.1x Accounting

Enabling AAA system accounting with 802.1x accounting allows system reload events to be sent to the accounting RADIUS server for logging. The server can then infer that all active 802.1x sessions are closed.

Because RADIUS uses the unreliable UDP transport protocol, accounting messages might be lost due to poor network conditions. If the switch does not receive the accounting response message from the RADIUS server after a configurable number of retransmissions of an accounting request, this system message appears:

```
Accounting message %s for session %s failed to receive Accounting Response.
```

When the stop message is not sent successfully, this message appears:

```
00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.
```

Note You must configure the RADIUS server to perform accounting tasks, such as logging start, stop, and interim-update messages and time stamps. To turn on these functions, enable logging of "Update/Watchdog packets from this AAA client" in your RADIUS server Network Configuration tab. Next, enable "CVS RADIUS Accounting" in your RADIUS server System Configuration tab.

Beginning in privileged EXEC mode, follow these steps to configure 802.1x accounting after AAA is enabled on your switch. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/3`	Specifies the port to be configured, and enter interface configuration mode.
Step 3	**aaa accounting dot1x default start-stop group radius** **Example:** `Switch(config-if)# aaa accounting dot1x default start-stop group radius`	Enables 802.1x accounting using the list of all RADIUS servers.
Step 4	**aaa accounting system default start-stop group radius** **Example:** `Switch(config-if)# aaa accounting system`	(Optional) Enables system accounting (using the list of all RADIUS servers) and generates system accounting reload event messages when the switch reloads.

	Command or Action	Purpose
	`default start-stop group radius`	
Step 5	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEc mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring a Guest VLAN

When you configure a guest VLAN, clients that are not 802.1x-capable are put into the guest VLAN when the server does not receive a response to its EAP request/identity frame. Clients that are 802.1x-capable but that fail authentication are not granted network access. The switch supports guest VLANs in single-host or multiple-hosts mode.

Beginning in privileged EXEC mode, follow these steps to configure a guest VLAN. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet2/0/2`	Specifies the port to be configured, and enter interface configuration mode.
Step 3	Use one of the following:	• Sets the port to access mode.

	Command or Action	Purpose
	• **switchport mode access** • **switchport mode private-vlan host** **Example:** `Switch(config-if)# switchport mode private-vlan host`	• Configures the Layer 2 port as a private-VLAN host port.
Step 4	**authentication event no-response action authorize vlan** *vlan-id* **Example:** `Switch(config-if)# authentication event no-response action authorize vlan 2`	Specifies an active VLAN as an 802.1x guest VLAN. The range is 1 to 4094. You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN or a voice VLAN as an 802.1x guest VLAN.
Step 5	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Configuring a Restricted VLAN

When you configure a restricted VLAN on a switch stack or a switch, clients that are IEEE 802.1x-compliant are moved into the restricted VLAN when the authentication server does not receive a valid username and password. The switch supports restricted VLANs only in single-host mode.

Beginning in privileged EXEC mode, follow these steps to configure a restricted VLAN. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet2/0/2`	Specifies the port to be configured, and enter interface configuration mode.
Step 3	Use one of the following:	• Sets the port to access mode.

	Command or Action	Purpose
	• **switchport mode access** • **switchport mode private-vlan host** **Example:** `Switch(config-if)# switchport mode access`	• Configures the Layer 2 port as a private-VLAN host port.
Step 4	**authentication port-control auto** **Example:** `Switch(config-if)# authentication port-control auto`	Enables 802.1x authentication on the port.
Step 5	**authentication event fail action authorize vlan** *vlan-id* **Example:** `Switch(config-if)# authentication event fail action authorize vlan 2`	Specifies an active VLAN as an 802.1x restricted VLAN. The range is 1 to 4094. You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN or a voice VLAN as an 802.1x restricted VLAN.
Step 6	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Configuring Number of Authentication Attempts on a Restricted VLAN

You can configure the maximum number of authentication attempts allowed before a user is assigned to the restricted VLAN by using the **authentication event retry** *retry count* interface configuration command. The range of allowable authentication attempts is 1 to 3. The default is 3 attempts.

Beginning in privileged EXEC mode, follow these steps to configure the maximum number of allowed authentication attempts. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *interface-id* **Example:**	Specifies the port to be configured, and enter interface configuration mode.

	Command or Action	Purpose
	`Switch(config)# interface gigabitethernet2/0/3`	
Step 3	Use one of the following: • **switchport mode access** • **switchport mode private-vlan host** **Example:** or `Switch(config-if)# switchport mode access`	• Sets the port to access mode. • Configures the Layer 2 port as a private-VLAN host port.
Step 4	**authentication port-control auto** **Example:** `Switch(config-if)# authentication port-control auto`	Enables 802.1x authentication on the port.
Step 5	**authentication event fail action authorize vlan** *vlan-id* **Example:** `Switch(config-if)# authentication event fail action authorize vlan 8`	Specifies an active VLAN as an 802.1x restricted VLAN. The range is 1 to 4094. You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN or a voice VLAN as an 802.1x restricted VLAN.
Step 6	**authentication event retry** *retry count* **Example:** `Switch(config-if)# authentication event retry 2`	Specifies a number of authentication attempts to allow before a port moves to the restricted VLAN. The range is 1 to 3, and the default is 3.
Step 7	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Configuring 802.1x Inaccessible Authentication Bypass with Critical Voice VLAN

Beginning in privileged EXEC mode, follow these steps to configure critical voice VLAN on a port and enable the inaccessible authentication bypass feature.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables AAA.
Step 3	**radius-server dead-criteria** {**time** *seconds* } [**tries** *number*] **Example:** `Switch(config)# radius-server dead-criteria time 20 tries 10`	Sets the conditions that determine when a RADIUS server is considered un-available or down (dead). • **time**— 1 to 120 seconds. The switch dynamically determines a default *seconds* value between 10 and 60. • **number**—1 to 100 tries. The switch dynamically determines a default **tries***number* between 10 and 100.
Step 4	**radius-serverdeadtime***minutes* **Example:** `Switch(config)# radius-server deadtime 60`	(Optional) Sets the number of minutes during which a RADIUS server is not sent requests. The range is from 0 to 1440 minutes (24 hours). The default is 0 minutes.
Step 5	**radius server** *server name* **Example:** `Switch(config)# radius server rsim address ipv4 124.2.2.12`	(Optional) Specifies the IP address of the RADIUS server.
Step 6	**address** {**ipv4** | **ipv6**} *ip address* **auth-port** *port_number* **acct-port** *port_number* **Example:** `Switch(config-radius-server)# address ipv4 10.0.1.2 auth-port 1550 acct-port 1560`	Configures the IP address for the RADIUS server.

	Command or Action	Purpose
Step 7	**key** *string* **Example:** `Switch(config-radius-server)# key rad123`	(Optional) Specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.
Step 8	**exit** **Example:** `Switch(config-radius-server)# exit`	Exits the RADIUS server mode and enters the global configuration mode.

Step 9	**dot1x critical** {**eapol** | **recovery delay** *milliseconds*}
	Example:
	`Switch(config)# dot1x critical eapol`
	`(config)# dot1x critical recovery delay 2000`
		(Optional) Configure the parameters for inaccessible authentication bypass:
		• **eapol**—Specify that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port.
		• **recovery delay***milliseconds*—Set the recovery delay period during which the switch waits to re-initialize a critical port when a RADIUS server that was unavailable becomes available. The range is from 1 to 10000 milliseconds. The default is 1000 milliseconds (a port can be re-initialized every second).

Step 10	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Specify the port to be configured, and enter interface configuration mode.
Step 11	**authentication event server dead action** {**authorize** | **reinitialize**} **vlan** *vlan-id*] **Example:** `Switch(config-if)# authentication event server dead action reinitialicze vlan 20`	Use these keywords to move hosts on the port if the RADIUS server is unreachable: • **authorize**—Move any new hosts trying to authenticate to the user-specified critical VLAN. • **reinitialize**—Move all authorized hosts on the port to the user-specified critical VLAN.

	Command or Action	Purpose
Step 12	**switchport voice vlan** *vlan-id* **Example:** `Switch(config-if)# switchport voice vlan`	Specifies the voice VLAN for the port. The voice VLAN cannot be the same as the critical data VLAN configured in Step 6.
Step 13	**authentication event server dead action authorize voice** **Example:** `Switch(config-if)# authentication event server dead action authorize voice`	Configures critical voice VLAN to move data traffic on the port to the voice VLAN if the RADIUS server is unreachable.
Step 14	**show authentication interface** *interface-id* **Example:** `Switch(config-if)# do show authentication interface gigabit 1/0/1`	(Optional) Verify your entries.
Step 15	**copy running-config startup-config** **Example:** `Switch(config-if)# do copy running-config startup-config`	(Optional) Verify your entries.

Example

To return to the RADIUS server default settings, use the **no radius-server dead-criteria**, the **no radius-server deadtime**, and the **no radius server** global configuration commands. To disable inaccessible authentication bypass, use the **no authentication event server dead action** interface configuration command. To disable critical voice VLAN, use the no **authentication event server dead action authorize voice** interface configuration command.

Example of Configuring Inaccessible Authentication Bypass

This example shows how to configure the inaccessible authentication bypass feature:

```
Switch(config)# radius-server dead-criteria time 30 tries 20
Switch(config)# radius-server deadtime 60
Switch(config)# radius server server1
Switch(config-radius-server)# address ipv4 172.29.36.49 acct-port 1618 auth-port 1612
Switch(config-radius-server)# key abc1234
Switch(config-radius-server)# exit
Switch(config)# dot1x critical eapol
```

```
Switch(config)# dot1x critical recovery delay 2000
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# dot1x critical
Switch(config-if)# dot1x critical recovery action reinitialize
Switch(config-if)# dot1x critical vlan 20
Switch(config-if)# end
```

Configuring 802.1x Authentication with WoL

Beginning in privileged EXEC mode, follow these steps to enable 802.1x authentication with WoL. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet2/0/3`	Specifies the port to be configured, and enter interface configuration mode.
Step 3	**authentication control-direction** {**both** | **in**} **Example:** `Switch(config-if)# authentication control-direction both`	Enables 802.1x authentication with WoL on the port, and use these keywords to configure the port as bidirectional or unidirectional. • **both**—Sets the port as bidirectional. The port cannot receive packets from or send packets to the host. By default, the port is bidirectional. • **in**—Sets the port as unidirectional. The port can send packets to the host but cannot receive packets from the host.
Step 4	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 5	**show authentication sessions interface** *interface-id* **Example:**	Verifies your entries.

	Command or Action	Purpose
	`Switch# show authentication sessions interface gigabitethernet2/0/3`	
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring MAC Authentication Bypass

Beginning in privileged EXEC mode, follow these steps to enable MAC authentication bypass. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet2/0/1`	Specifies the port to be configured, and enter interface configuration mode.
Step 3	**authentication port-control auto** **Example:** `Switch(config-if)# authentication port-control auto`	Enables 802.1x authentication on the port.
Step 4	**mab** [**eap**] **Example:** `Switch(config-if)# mab`	Enables MAC authentication bypass. (Optional) Use the **eap** keyword to configure the switch to use EAP for authorization.
Step 5	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Switch(config-if)# end`	

Configuring 802.1x User Distribution

Beginning in privileged EXEC mode, follow these steps to configure a VLAN group and to map a VLAN to it:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**vlan group** *vlan-group-name* **vlan-list** *vlan-list* **Example:** `Switch(config)# vlan group eng-dept vlan-list 10`	Configures a VLAN group, and maps a single VLAN or a range of VLANs to it.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 4	**no vlan group** *vlan-group-name* **vlan-list** *vlan-list* **Example:** `Switch(config)# no vlan group eng-dept vlan-list 10`	Clears the VLAN group configuration or elements of the VLAN group configuration.

Example of Configuring VLAN Groups

This example shows how to configure the VLAN groups, to map the VLANs to the groups, to and verify the VLAN group configurations and mapping to the specified VLANs:

```
Switch(config)# vlan group eng-dept vlan-list 10

Switch(config)# show vlan group group-name eng-dept
Group Name                      Vlans Mapped
-------------                   --------------
```

```
eng-dept                        10

Switch(config)# show dot1x vlan-group all
Group Name                      Vlans Mapped
-------------                   --------------
eng-dept                        10
hr-dept                         20
```

This example shows how to add a VLAN to an existing VLAN group and to verify that the VLAN was added:

```
Switch(config)# vlan group eng-dept vlan-list 30
Switch(config)# show vlan group eng-dept
Group Name                      Vlans Mapped
-------------                   --------------
eng-dept                        10,30
```

This example shows how to remove a VLAN from a VLAN group:

```
Switch# no vlan group eng-dept vlan-list 10
```

This example shows that when all the VLANs are cleared from a VLAN group, the VLAN group is cleared:

```
Switch(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.

Switch(config)# show vlan group group-name eng-dept
```

This example shows how to clear all the VLAN groups:

```
Switch(config)# no vlan group end-dept vlan-list all
Switch(config)# show vlan-group all
```

For more information about these commands, see the *Cisco IOS Security Command Reference.*

Configuring NAC Layer 2 802.1x Validation

You can configure NAC Layer 2 802.1x validation, which is also referred to as 802.1x authentication with a RADIUS server.

Beginning in privileged EXEC mode, follow these steps to configure NAC Layer 2 802.1x validation. The procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet2/0/3`	Specifies the port to be configured, and enter interface configuration mode.
Step 3	**switchport mode access** **Example:** `Switch(config-if)# switchport mode access`	Sets the port to access mode only if you configured the RADIUS server.
Step 4	**authentication event no-response action authorize vlan** *vlan-id* **Example:** `Switch(config-if)# authentication event no-response action authorize vlan 8`	Specifies an active VLAN as an 802.1x guest VLAN. The range is 1 to 4094. You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN, or a voice VLAN as an 802.1x guest VLAN.
Step 5	**authentication periodic** **Example:** `Switch(config-if)# authentication periodic`	Enables periodic re-authentication of the client, which is disabled by default.
Step 6	**authentication timer reauthenticate** **Example:** `Switch(config-if)# authentication timer reauthenticate`	Sets re-authentication attempt for the client (set to one hour). This command affects the behavior of the switch only if periodic re-authentication is enabled.
Step 7	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 8	**show authentication sessions interface** *interface-id* **Example:** `Switch# show authentication sessions interface gigabitethernet2/0/3`	Verifies your entries.

	Command or Action	Purpose
Step 9	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Limiting Login for Users

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables the authentication, authorization, and accounting (AAA) access control model.
Step 4	**aaa authentication login default local** **Example:** `Device(config)# aaa authentication login default local`	Sets the authentication, authorization, and accounting (AAA) authentication by using the default authentication methods.
Step 5	**aaa authentication rejected** *n* **in** *m* **ban** *x* **Example:** `Device(config)# aaa authentication rejected 3 in 20 ban 300`	Configures the time period for which an user is blocked, if the user fails to successfully login within the specified time and login attempts. • *n*—Specifies the number of times a user can try to login. • *m*—Specifies the number of seconds within which an user can try to login. • *x*—Specifies the time period an user is banned if the user fails to successfully login.
Step 6	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 7	**show aaa local user blocked** **Example:** `Device# show aaa local user blocked`	Displays the list of local users who were blocked.
Step 8	**clear aaa local user blocked username** *username* **Example:** `Device# clear aaa local user blocked username user1`	Clears the information about the blocked local user.

Example

The following is sample output from the **show aaa local user blocked** command:

```
Device# show aaa local user blocked

       Local-user                 State

       user1                      Watched (till 11:34:42 IST Feb 5 2015)
```

Configuring an Authenticator Switch with NEAT

Configuring this feature requires that one switch outside a wiring closet is configured as a supplicant and is connected to an authenticator switch.

Note The *cisco-av-pairs* must be configured as *device-traffic-class=switch* on the ACS, which sets the interface as a trunk after the supplicant is successfully authenticated.

Beginning in privileged EXEC mode, follow these steps to configure a switch as an authenticator:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**cisp enable** **Example:**	Enables CISP.

	Command or Action	Purpose
	`Switch(config)# cisp enable`	
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet2/0/1`	Specifies the port to be configured, and enter interface configuration mode.
Step 4	**switchport mode access** **Example:** `Switch(config-if)# switchport mode access`	Sets the port mode to **access**.
Step 5	**authentication port-control auto** **Example:** `Switch(config-if)# authentication port-control auto`	Sets the port-authentication mode to auto.
Step 6	**dot1x pae authenticator** **Example:** `Switch(config-if)# dot1x pae authenticator`	Configures the interface as a port access entity (PAE) authenticator.
Step 7	**spanning-tree portfast** **Example:** `Switch(config-if)# spanning-tree portfast trunk`	Enables Port Fast on an access port connected to a single workstation or server..
Step 8	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 9	**show running-config interface** *interface-id* **Example:** `Switch# show running-config interface gigabitethernet2/0/1`	Verifies your configuration.

	Command or Action	Purpose
Step 10	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file. **Note** Saving changes to the configuration file will mean that the authenticator interface will continue to be in trunk mode after reload. If you want the authenticator interface to remain as an access port, do not save your changes to the configuration file.

Configuring a Supplicant Switch with NEAT

Beginning in privileged EXEC mode, follow these steps to configure a switch as a supplicant:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**cisp enable** **Example:** `Switch(config)# cisp enable`	Enables CISP.
Step 3	**dot1x credentials** *profile* **Example:** `Switch(config)# dot1x credentials test`	Creates 802.1x credentials profile. This must be attached to the port that is configured as supplicant.
Step 4	**username** *suppswitch* **Example:** `Switch(config)# username suppswitch`	Creates a username.
Step 5	**password** *password* **Example:** `Switch(config)# password myswitch`	Creates a password for the new username.

	Command or Action	Purpose
Step 6	**dot1x supplicant force-multicast** **Example:** `Switch(config)# dot1x supplicant force-multicast`	Forces the switch to send only multicast EAPOL packets when it receives either unicast or multicast packets. This also allows NEAT to work on the supplicant switch in all host modes.
Step 7	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/1`	Specifies the port to be configured, and enter interface configuration mode.
Step 8	**switchport trunk encapsulation dot1q** **Example:** `Switch(config-if)# switchport trunk encapsulation dot1q`	Sets the port to trunk mode.
Step 9	**switchport mode trunk** **Example:** `Switch(config-if)# switchport mode trunk`	Configures the interface as a VLAN trunk port.
Step 10	**dot1x pae supplicant** **Example:** `Switch(config-if)# dot1x pae supplicant`	Configures the interface as a port access entity (PAE) supplicant.
Step 11	**dot1x credentials** *profile-name* **Example:** `Switch(config-if)# dot1x credentials test`	Attaches the 802.1x credentials profile to the interface.
Step 12	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 13	**show running-config interface** *interface-id* **Example:**	Verifies your configuration.

	Command or Action	Purpose
	`Switch# show running-config interface gigabitethernet1/0/1`	
Step 14	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.
Step 15	Configuring NEAT with Auto Smartports Macros	You can also use an Auto Smartports user-defined macro instead of the switch VSA to configure the authenticator switch. For more information, see the *Auto Smartports Configuration Guide* for this release.

Configuring 802.1x Authentication with Downloadable ACLs and Redirect URLs

In addition to configuring 802.1x authentication on the switch, you need to configure the ACS. For more information, see the *Configuration Guide for Cisco Secure ACS 4.2*: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/configuration/guide/acs_config.pdf

Note You must configure a downloadable ACL on the ACS before downloading it to the switch.

After authentication on the port, you can use the **show ip access-list** privileged EXEC command to display the downloaded ACLs on the port.

Configuring Downloadable ACLs

The policies take effect after client authentication and the client IP address addition to the IP device tracking table. The switch then applies the downloadable ACL to the port.

Beginning in privileged EXEC mode:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ip device tracking** **Example:**	Sets the ip device tracking table.

	Command or Action	Purpose
	`Switch(config)# ip device tracking`	
Step 3	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables AAA.
Step 4	**aaa authorization network default local group radius** **Example:** `Switch(config)# aaa authorization network default local group radius`	Sets the authorization method to local. To remove the authorization method, use the **no aaa authorization network default local group radius** command.
Step 5	**radius-server vsa send authentication** **Example:** `Switch(config)# radius-server vsa send authentication`	Configures the radius vsa send authentication.
Step 6	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet2/0/4`	Specifies the port to be configured, and enter interface configuration mode.
Step 7	**ip access-group** *acl-id* **in** **Example:** `Switch(config-if)# ip access-group default_acl in`	Configures the default ACL on the port in the input direction. **Note** The *acl-id* is an access list name or number.
Step 8	**show running-config interface** *interface-id* **Example:** `Switch(config-if)# show running-config interface gigabitethernet2/0/4`	Verifies your configuration.
Step 9	**copy running-config startup-config** **Example:** `Switch# copy running-config`	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	`startup-config`	

Configuring a Downloadable Policy

Beginning in privileged EXEC mode:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**access-list** *access-list-number* **{ deny | permit } { hostname | any | host } log** **Example:** `Switch(config)# access-list 1 deny any log`	Defines the default port ACL. The access-list-number is a decimal number from 1 to 99 or 1300 to 1999. Enter **deny** or **permit** to specify whether to deny or permit access if conditions are matched. The source is the source address of the network or host that sends a packet, such as this: • **hostname**: The 32-bit quantity in dotted-decimal format. • **any**: The keyword any as an abbreviation for source and source-wildcard value of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard value. • **host**: The keyword host as an abbreviation for source and source-wildcard of source 0.0.0.0. (Optional) Applies the source-wildcard wildcard bits to the source. (Optional) Enters log to cause an informational logging message about the packet that matches the entry to be sent to the console.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface`	Enters interface configuration mode.

	Command or Action	Purpose
	`gigabitethernet2/0/2`	
Step 4	**ip access-group** *acl-id* **in** **Example:** `Switch(config-if)# ip access-group default_acl in`	Configures the default ACL on the port in the input direction. **Note** The acl-id is an access list name or number.
Step 5	**exit** **Example:** `Switch(config-if)# exit`	Returns to global configuration mode.
Step 6	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables AAA.
Step 7	**aaa authorization network default group radius** **Example:** `Switch(config)# aaa authorization network default group radius`	Sets the authorization method to local. To remove the authorization method, use the **no aaa authorization network default group radius** command.
Step 8	**ip device tracking** **Example:** `Switch(config)# ip device tracking`	Enables the IP device tracking table. To disable the IP device tracking table, use the **no ip device tracking** global configuration commands.
Step 9	**ip device tracking probe** [**count** | **interval** | **use-svi**] **Example:** `Switch(config)# ip device tracking probe count`	(Optional) Configures the IP device tracking table: • **count** *count*—Sets the number of times that the switch sends the ARP probe. The range is from 1 to 5. The default is 3. • **interval** *interval*—Sets the number of seconds that the switch waits for a response before resending the ARP probe. The range is from 30 to 300 seconds. The default is 30 seconds. • **use-svi**—Uses the switch virtual interface (SVI) IP address as source of ARP probes.

	Command or Action	Purpose
Step 10	**radius-server vsa send authentication** **Example:** `Switch(config)# radius-server vsa send authentication`	Configures the network access server to recognize and use vendor-specific attributes. **Note** The downloadable ACL must be operational.
Step 11	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Configuring VLAN ID-based MAC Authentication

Beginning in privileged EXEC mode, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**mab request format attribute 32 vlan access-vlan** **Example:** `Switch(config)# mab request format attribute 32 vlan access-vlan`	Enables VLAN ID-based MAC authentication.
Step 3	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Flexible Authentication Ordering

The examples used in the instructions below changes the order of Flexible Authentication Ordering so that MAB is attempted before IEEE 802.1X authentication (dot1x). MAB is configured as the first authentication method, so MAB will have priority over all other authentication methods.

Note Before changing the default order and priority of these authentication methods, however, you should understand the potential consequences of those changes. See http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/application_note_c27-573287_ps6638_Products_White_Paper.html for details.

Beginning in privileged EXEC mode, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Specifies the port to be configured, and enter interface configuration mode.
Step 3	**switchport mode access** **Example:** `Switch(config-if)# switchport mode access`	Sets the port to access mode only if you previously configured the RADIUS server.
Step 4	**authentication order** [**dot1x** | **mab**] | {**webauth**} **Example:** `Switch(config-if)# authentication order mab dot1x`	(Optional) Sets the order of authentication methods used on a port.
Step 5	**authentication priority** [**dot1x** | **mab**] | {**webauth**} **Example:** `Switch(config-if)# authentication priority mab dot1x`	(Optional) Adds an authentication method to the port-priority list.
Step 6	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Switch(config-if)# end`	

Configuring Open1x

Beginning in privileged EXEC mode, follow these steps to enable manual control of the port authorization state:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 1/0/1`	Specifies the port to be configured, and enter interface configuration mode.
Step 3	**switchport mode access** **Example:** `Switch(config-if)# switchport mode access`	Sets the port to access mode only if you configured the RADIUS server.
Step 4	**authentication control-direction** {**both** | **in**} **Example:** `Switch(config-if)# authentication control-direction both`	(Optional) Configures the port control as unidirectional or bidirectional.
Step 5	**authentication fallback** *name* **Example:** `Switch(config-if)# authentication fallback profile1`	(Optional) Configures a port to use web authentication as a fallback method for clients that do not support 802.1x authentication.

	Command or Action	Purpose
Step 6	**authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**] **Example:** `Switch(config-if)# authentication host-mode multi-auth`	(Optional) Sets the authorization manager mode on a port.
Step 7	**authentication open** **Example:** `Switch(config-if)# authentication open`	(Optional) Enables or disable open access on a port.
Step 8	**authentication order** [**dot1x** | **mab**] | {**webauth**} **Example:** `Switch(config-if)# authentication order dot1x webauth`	(Optional) Sets the order of authentication methods used on a port.
Step 9	**authentication periodic** **Example:** `Switch(config-if)# authentication periodic`	(Optional) Enables or disable reauthentication on a port.
Step 10	**authentication port-control** {**auto** | **force-authorized** | **force-un authorized**} **Example:** `Switch(config-if)# authentication port-control auto`	(Optional) Enables manual control of the port authorization state.
Step 11	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Disabling 802.1x Authentication on the Port

You can disable 802.1x authentication on the port by using the **no dot1x pae** interface configuration command.

Beginning in privileged EXEC mode, follow these steps to disable 802.1x authentication on the port. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet2/0/1`	Specifies the port to be configured, and enter interface configuration mode.
Step 3	**switchport mode access** **Example:** `Switch(config-if)# switchport mode access`	(Optional) Sets the port to access mode only if you configured the RADIUS server.
Step 4	**no dot1x pae authenticator** **Example:** `Switch(config-if)# no dot1x pae authenticator`	Disables 802.1x authentication on the port.
Step 5	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Resetting the 802.1x Authentication Configuration to the Default Values

Beginning in privileged EXEC mode, follow these steps to reset the 802.1x authentication configuration to the default values. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/2`	Enters interface configuration mode, and specify the port to be configured.
Step 3	**dot1x default** **Example:** `Switch(config-if)# dot1x default`	Resets the 802.1x parameters to the default values.
Step 4	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Monitoring 802.1x Statistics and Status

Table 75: Privileged EXEC show Commands

Command	Purpose
show dot1x all statistics	Displays 802.1x statistics for all ports
show dot1x interface *interface-id* **statistics**	Displays 802.1x statistics for a specific port
show dot1x all [**count** | **details** | **statistics** | **summary**]	Displays the 802.1x administrative and operational status for a switch
show dot1x interface *interface-id*	Displays the 802.1x administrative and operational status for a specific port

Table 76: Global Configuration Commands

Command	Purpose
no dot1x logging verbose	Filters verbose 802.1x authentication messages (beginning with Cisco IOS Release 12.2(55)SE)

For detailed information about the fields in these displays, see the command reference for this release.

Additional References for IEEE 802.1x Port-Based Authentication

Related Documents

Related Topic	Document Title
Configuring Identity Control policies and Identity Service templates for Session Aware networking.	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.htm
Configuring RADIUS, TACACS+, Secure Shell, 802.1X and AAA.	Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switch http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secuser-xe-3se-3850-l

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

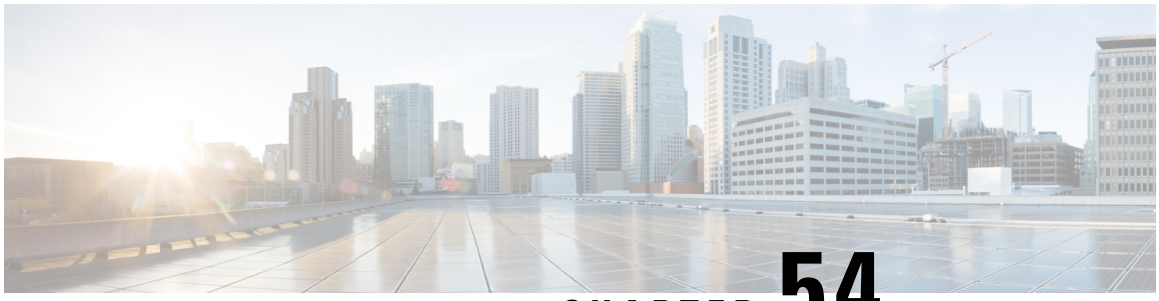
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for 802.1x Port-Based Authentication

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.
	Supports the use of same authorization methods on all the Catalyst switches in a network.
	Supports filtering verbose system messages from the authentication manager.



CHAPTER 54

Configuring MACsec Encryption

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restriction for MACSec Encryption

- While configuring MACsec MKA using EAP-TLS, MACsec secure channels encrypt counters wont increment before first Rekey.

Information About MACsec Encryption

This chapter describes how to configure Media Access Control Security (MACsec) encryption on the Catalyst switches. MACsec is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices. The switch also supports MACsec link layer switch-to-switch security by using Cisco TrustSec Network Device Admission Control (NDAC) and the Security Association Protocol (SAP) key exchange. Link layer security can include both packet authentication between switches and MACsec encryption between switches (encryption is optional).

Note MACsec is not supported on switches running the NPE or the LAN base image.

All downlink ports on the switch can run Cisco TrustSec MACsec link layer switch-to-switch security.

Table 77: MACsec Support on Switch Ports

Interface	**Connections**	MACsec support
Switchports connected to other switches	Switch-to-switch	Cisco TrustSec NDAC MACsec

Cisco TrustSec and Cisco SAP are meant only for switch-to-switch links and are not supported on switch ports connected to end hosts, such as PCs or IP phones. Cisco NDAC and SAP are mutually exclusive with Network Edge Access Topology (NEAT), which is used for compact switches to extend security outside the wiring closet.

Media Access Control Security and MACsec Key Agreement

MACsec, defined in 802.1AE, provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys. MKA and MACsec are implemented after successful authentication using the 802.1x Extensible Authentication Protocol (EAP-TLS) or Pre Shared Key (PSK) framework.

A switch using MACsec accepts either MACsec or non-MACsec frames, depending on the policy associated with the MKA peer. MACsec frames are encrypted and protected with an integrity check value (ICV). When the switch receives frames from the MKA peer, it decrypts them and calculates the correct ICV by using session keys provided by MKA. The switch compares that ICV to the ICV within the frame. If they are not identical, the frame is dropped. The switch also encrypts and adds an ICV to any frames sent over the secured port (the access point used to provide the secure MAC service to a MKA peer) using the current session key.

The MKA Protocol manages the encryption keys used by the underlying MACsec protocol. The basic requirements of MKA are defined in 802.1x-REV. The MKA Protocol extends 802.1x to allow peer discovery with confirmation of mutual authentication and sharing of MACsec secret keys to protect data exchanged by the peers.

The EAP framework implements MKA as a newly defined EAP-over-LAN (EAPOL) packet. EAP authentication produces a master session key (MSK) shared by both partners in the data exchange. Entering the EAP session ID generates a secure connectivity association key name (CKN). The switch acts as the authenticator for both uplink and downlink; and acts as the key server for downlink. It generates a random secure association key (SAK), which is sent to the client partner. The client is never a key server and can only interact with a single MKA entity, the key server. After key derivation and generation, the switch sends periodic transports to the partner at a default interval of 2 seconds.

The packet body in an EAPOL Protocol Data Unit (PDU) is referred to as a MACsec Key Agreement PDU (MKPDU). MKA sessions and participants are deleted when the MKA lifetime (6 seconds) passes with no MKPDU received from a participant. For example, if a MKA peer disconnects, the participant on the switch continues to operate MKA until 6 seconds have elapsed after the last MKPDU is received from the MKA peer.

Note Integrity check value (ICV) indicator in MKPDU is optional. ICV is not optional when the traffic is encrypted.

Prior to Cisco IOS XE Fuji 16.8.1a, should-secure was supported for MKA and SAP. With should-secure enabled, if the peer is configured for MACsec, the data traffic is encrypted, otherwise it is sent in clear text. Starting with Cisco IOS XE Fuji 16.8.1a, must-secure support is enabled on both the ingress and the egress. Must-secure is supported for MKA and SAP. With must-secure enabled, only EAPoL traffic will not be encrypted. The rest of the traffic will be encrypted. Unencrypted packets are dropped.

Note Must-secure mode is enabled by default.

MKA Policies

To enable MKA on an interface, a defined MKA policy should be applied to the interface. Removing the MKA policy disables MKA on that interface. You can configure these options:

- Policy name, not to exceed 16 ASCII characters.
- Confidentiality (encryption) offset of 0, 30, or 50 bytes for each physical interface
- Replay protection. You can configure MACsec window size, as defined by the number of out-of-order frames that are accepted. This value is used while installing the security associations in the MACsec. A value of 0 means that frames are accepted only in the correct order.

Virtual Ports

You use virtual ports for multiple secured connectivity associations on a single physical port. Each connectivity association (pair) represents a virtual port, with a maximum of two virtual ports per physical port. Only one of the two virtual ports can be part of a data VLAN; the other must externally tag its packets for the voice VLAN. You cannot simultaneously host secured and unsecured sessions in the same VLAN on the same port. Because of this limitation, 802.1x multiple authentication mode is not supported.

The exception to this limitation is in multiple-host mode when the first MACsec supplicant is successfully authenticated and connected to a hub that is connected to the switch. A non-MACsec host connected to the hub can send traffic without authentication because it is in multiple-host mode. We do not recommend using multi-host mode because after the first successful client, authentication is not required for other clients.

Virtual ports represent an arbitrary identifier for a connectivity association and have no meaning outside the MKA Protocol. A virtual port corresponds to a separate logical port ID. Valid port IDs for a virtual port are 0x0002 to 0xFFFF. Each virtual port receives a unique secure channel identifier (SCI) based on the MAC address of the physical interface concatenated with a 16-bit port ID.

MACsec and Stacking

A Switch stack master running MACsec maintains the configuration files that show which ports on a member switch support MACsec. The stack master performs these functions:

- Processes secure channel and secure association creation and deletion
- Sends secure association service requests to the stack members.

- Processes packet number and replay-window information from local or remote ports and notifies the key management protocol.
- Sends MACsec initialization requests with the globally configured options to new switches that are added to the stack.
- Sends any per-port configuration to the member switches.

A member switch performs these functions:

- Processes MACsec initialization requests from the stack master.
- Processes MACsec service requests sent by the stack master.
- Sends information about local ports to the stack master.

In case of a stack master changeover, all secured sessions are brought down and then reestablished. The authentication manager recognizes any secured sessions and initiates teardown of these sessions.

Note If you are using 1G SFP modules for inter switch connection, change system MTU to 1550 byte to ensure support of MACsec overhead.

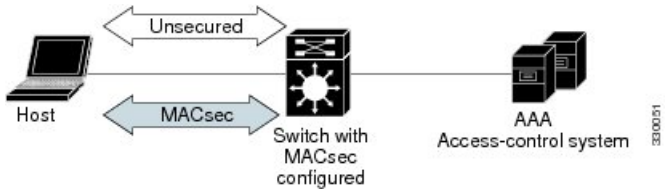
MACsec, MKA and 802.1x Host Modes

You can use MACsec and the MKA Protocol with 802.1x single-host mode or Multi Domain Authentication (MDA) mode. Multiple authentication mode is not supported.

Single-Host Mode

The figure shows how a single EAP authenticated session is secured by MACsec by using MKA

Figure 63: MACsec in Single-Host Mode with a Secured Data Session



MKA Statistics

Some MKA counters are aggregated globally, while others are updated both globally and per session. You can also obtain information about the status of MKA sessions.

This is an example of the**show mka statistics** command output:

```
SWitch# show mka statistics
MKA Global Statistics
=====================
MKA Session Totals
Secured..................... 32
Reauthentication Attempts.. 31

Deleted (Secured)......... 1
Keepalive Timeouts........ 0
```

```
CA Statistics
Pairwise CAKs Derived...... 32
Pairwise CAK Rekeys........ 31
Group CAKs Generated....... 0
Group CAKs Received........ 0

SA Statistics
SAKs Generated............. 32
SAKs Rekeyed............... 31
SAKs Received.............. 0
SAK Responses Received..... 32


MKPDU Statistics
MKPDUs Validated & Rx...... 580
"Distributed SAK"..... 0
"Distributed CAK"..... 0
MKPDUs Transmitted......... 597
"Distributed SAK"..... 32
"Distributed CAK"..... 0

MKA Error Counter Totals
========================

Bring-up Failures.................. 0
Reauthentication Failures.......... 0

SAK Failures
SAK Generation.................. 0
Hash Key Generation............. 0
SAK Encryption/Wrap............. 0
SAK Decryption/Unwrap........... 0


CA Failures
Group CAK Generation............ 0
Group CAK Encryption/Wrap....... 0
Group CAK Decryption/Unwrap..... 0
Pairwise CAK Derivation......... 0
CKN Derivation.................. 0
ICK Derivation.................. 0
KEK Derivation.................. 0
Invalid Peer MACsec Capability.. 2

MACsec Failures
Rx SC Creation.................. 0
Tx SC Creation.................. 0
Rx SA Installation.............. 0
Tx SA Installation.............. 0

MKPDU Failures
MKPDU Tx........................ 0
MKPDU Rx Validation............. 0
MKPDU Rx Bad Peer MN............ 0
MKPDU Rx Non-recent Peerlist MN.. 0
```

Configuring MKA and MACsec

Default MACsec MKA Configuration

MACsec is disabled. No MKA policies are configured.

Related Topics

Configuring MACsec on an Interface, on page 1069
Configuring an MKA Policy, on page 1068
Example: Configuring MACsec on an Interface, on page 1078

Configuring an MKA Policy

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mka policy** *policy name*	Identify an MKA policy, and enter MKA policy configuration mode. The maximum policy name length is 16 characters.
Step 3	**confidentiality-offset** *Offset value*	Set the Confidentiality (encryption) offset for each physical interface **Note** Offset Value can be 0, 30 or 50. If you are using Anyconnect on the client, it is recommended to use Offset 0.
Step 4	**replay-protection window-size** *frames*	Enable replay protection, and configure the window size in number of frames. The range is from 0 to 4294967295. The default window size is 0. Entering a window size of 0 is not the same as entering the **no replay-protection command**. Configuring a window size of 0 uses replay protection with a strict ordering of frames. Entering **no replay-protection** turns off MACsec replay-protection.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show mka policy**	Verify your entries.

Example

This example configures the MKA policy *relay-policy*:

```
Switch(config)# mka policy replay-policy
Switch(config-mka-policy)# confidentiality-offset 0
Switch(config-mka-policy)# replay-protection window-size 300
Switch(config-mka-policy)# end
```

Related Topics

Default MACsec MKA Configuration, on page 1067
Example: Configuring MACsec on an Interface, on page 1078

Configuring MACsec on an Interface

Follow these steps to configure MACsec on an interface with one MACsec session for voice and one for data:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id*	Identify the MACsec interface, and enter interface configuration mode. The interface must be a physical interface.
Step 4	**switchport access vlan***vlan-id*	Configure the access VLAN for the port.
Step 5	**switchport mode access**	Configure the interface as an access port.
Step 6	**macsec**	Enable 802.1ae MACsec on the interface.
Step 7	**authentication event linksec fail action authorize vlan** *vlan-id*	(Optional) Specify that the switch processes authentication link-security failures resulting from unrecognized user credentials by authorizing a restricted VLAN on the port after a failed authentication attempt.
Step 8	**authentication host-mode multi-domain**	Configure authentication manager mode on the port to allow both a host and a voice device to be authenticated on the 802.1x-authorized port. If not configured, the default host mode is single.
Step 9	**authentication linksec policy must-secure**	Set the LinkSec security policy to secure the session with MACsec if the peer is available. If not set, the default is *should secure*.
Step 10	**authentication port-control auto**	Enable 802.1x authentication on the port. The port changes to the authorized or unauthorized

	Command or Action	Purpose
		state based on the authentication exchange between the switch and the client.
Step 11	**authentication periodic**	Enable or Disable Reauthentication for this port .
Step 12	**authentication timer reauthenticate**	Enter a value between 1 and 65535. Obtains re-authentication timeout value from the server.
Step 13	**authentication violation protect**	Configure the port to drop unexpected incoming MAC addresses when a new device connects to a port or when a device connects to a port after the maximum number of devices are connected to that port. If not configured, the default is to shut down the port.
Step 14	**mka policy** *policy name*	Apply an existing MKA protocol policy to the interface, and enable MKA on the interface. If no MKA policy was configured (by entering the **mka policy** global configuration command), you must apply the MKA default policy to the interface by entering the **mka default-policy** interface configuration command
Step 15	**dot1x pae authenticator**	Configure the port as an 802.1x port access entity (PAE) authenticator.
Step 16	**spanning-tree portfast**	Enable spanning tree Port Fast on the interface in all its associated VLANs. When Port Fast feature is enabled, the interface changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes
Step 17	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 18	**show authentication session interface** *interface-id*	Verify the authorized session security status.
Step 19	**show authentication session interface** *interface-id* details	Verify the details of the security status of the authorized session.
Step 20	**show macsec interface** *interface-id*	Verify MacSec status on the interface.
Step 21	**show mka sessions**	Verify the established mka sessions.

	Command or Action	Purpose
Step 22	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Default MACsec MKA Configuration, on page 1067
Example: Configuring MACsec on an Interface, on page 1078

Information About Cisco TrustSec

The table below lists the TrustSec features to be eventually implemented on TrustSec-enabled Cisco switches. Successive general availability releases of TrustSec will expand the number of switches supported and the number of TrustSec features supported per switch.

Cisco TrustSec Feature	Description
802.1AE Tagging (MACsec)	Protocol for IEEE 802.1AE-based wire-rate hop-to-hop Layer 2 encryption. Between MACsec-capable devices, packets are encrypted on egress from the transmitting device, decrypted on ingress to the receiving device, and in the clear within the devices. This feature is only available between TrustSec hardware-capable devices. **Note** This feature is not supported on Catalyst 3850 and Catalyst 3650 switches with Cisco IOS XE Denali 16.1.1
Endpoint Admission Control (EAC)	EAC is an authentication process for an endpoint user or a device connecting to the TrustSec domain. Usually EAC takes place at the access level switch. Successful authentication and authorization in the EAC process results in Security Group Tag assignment for the user or device. Currently EAC can be 802.1X, MAC Authentication Bypass (MAB), and Web Authentication Proxy (WebAuth).

Cisco TrustSec Feature	Description
Network Device Admission Control (NDAC)	NDAC is an authentication process where each network device in the TrustSec domain can verify the credentials and trustworthiness of its peer device. NDAC utilizes an authentication framework based on IEEE 802.1X port-based authentication and uses EAP-FAST as its EAP method. Successful authentication and authorization in NDAC process results in Security Association Protocol negotiation for IEEE 802.1AE encryption.
Security Group Access Control List (SGACL)	A Security Group Access Control List (SGACL) associates a Security Group Tag with a policy. The policy is enforced upon SGT-tagged traffic egressing the TrustSec domain. In Cisco IOS XE Fuji 16.8.1, IPv6 support was enabled for SGACL enforcement and logging of VRF name was enabled in SGACL logs.
Security Association Protocol (SAP)	After NDAC authentication, the Security Association Protocol (SAP) automatically negotiates keys and the cipher suite for subsequent MACSec link encryption between TrustSec peers. SAP is defined in IEEE 802.11i. **Note** This feature is not supported on Catalyst 3850 and Catalyst 3650 switches with Cisco IOS XE Denali 16.1.1
Security Group Tag (SGT)	An SGT is a 16-bit single label indicating the security classification of a source in the TrustSec domain. It is appended to an Ethernet frame or an IP packet. In Cisco IOS XE Fuji 16.8.1, Layer 2 Inline Tagging is supported for IPv6 multicast traffic with unicast source IPv6 addresses.
SGT Exchange Protocol (SXP)	Security Group Tag Exchange Protocol (SXP). With SXP, devices that are not TrustSec-hardware-capable can receive SGT attributes for authenticated users and devices from the Cisco Identity Services Engine (ISE) or the Cisco Secure Access Control System (ACS). The devices can then forward a sourceIP-to-SGT binding to a TrustSec-hardware-capable device will tag the source traffic for SGACL enforcement.

When both ends of a link support 802.1AE MACsec, SAP negotiation occurs. An EAPOL-key exchange occurs between the supplicant and the authenticator to negotiate a cipher suite, exchange security parameters, and manage keys. Successful completion of these tasks results in the establishment of a security association (SA).

Depending on your software version and licensing and link hardware support, SAP negotiation can use one of these modes of operation:

- Galois Counter Mode (GCM)—authentication and encryption
- GCM authentication (GMAC)— GCM authentication, no encryption
- No Encapsulation—no encapsulation (clear text)
- Null—encapsulation, no authentication or encryption

Related Topics

Configuring Cisco TrustSec MACsec, on page 1073

Configuring Cisco TrustSec MACsec

Related Topics

Information About Cisco TrustSec , on page 1071

Configuring Cisco TrustSec Credentials on the Switch

To enable Cisco TrustSec features, you must create Cisco TrustSec credentials on the switch to use in other TrustSec configurations. Beginning in privilege EXEC mode, follow these steps to configure Cisco TrustSec credentials.

Procedure

	Command or Action	Purpose
Step 1	**cts credentials id** *device-id* **password** *cts-password* **Example:** `Switch# cts credentials id trustsec password mypassword`	Specifies the Cisco TrustSec credentials for this switch to use when authenticating with other Cisco TrustSec devices with EAP-FAST. • **id** *device-id*—Specifies a Cisco TrustSec device ID for the switch. The device-id argument has a maximum length of 32 characters and is case sensitive • **password** *cts-password*—Specifies the Cisco TrustSec password for the device.
Step 2	**show cts credentials** **Example:** `Switch# show cts credentials`	(Optional) Displays Cisco TrustSec credentials configured on the switch.
Step 3	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Example

To delete the Cisco TrustSec credentials, enter the **clear cts credentials** privileged EXEC command.

This example shows how to create Cisco TrustSec credentials.

```
Switch# cts credentials id trustsec password mypassword
CTS device ID and password have been inserted in the local keystore. Please make
sure that the same ID and password are configured in the server database.

Switch# show cts credentials
CTS password is defined in keystore, device-id = trustsec
```

What to do next

Before you configure Cisco TrustSec MACsec authentication, you should configure Cisco TrustSec seed and non-seed devices. For 802.1x mode, you must configure at least one seed device, that device closest to the access control system (ACS). See this section in the Cisco TrustSec Configuration Guide:http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/ident-conn_config.html

Configuring Cisco TrustSec Switch-to-Switch Link Security in 802.1x Mode

Before you begin

You enable Cisco TrustSec link layer switch-to-switch security on an interface that connects to another Cisco TrustSec device. When configuring Cisco TrustSec in 802.1x mode on an interface, follow these guidelines:

- To use 802.1x mode, you must globally enable 802.1x on each device. For more information 802.1x, see the Configuring IEEE 802.1x Port-Based Authentication chapter.
- If you select GCM as the SAP operating mode, you must have a MACsec encryption software license from Cisco. MACsec is supported on Catalyst 3850 and 3650 universal IP Services and IP Base licenses . It is not supported with the NPE license or with a LAN base service image.

  If you select GCM without the required license, the interface is forced to a link-down state.

Beginning in privilege EXEC mode, follow these steps to configure Cisco TrustSec switch-to-switch link layer security with 802.1x:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface tengigabitethernet 1/1/2`	**Note** Enters interface configuration mode.

	Command or Action	Purpose
Step 3	**cts dot1x** **Example:** `Switch(config-if)# cts dot1x`	Configures the interface to perform NDAC authentication.
Step 4	**sap mode-list***mode1* [*mode2* [*mode3* [*mode4*]]] **Example:** `Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt null no-encap`	(Optional) Configures the SAP operation mode on the interface. The interface negotiates with the peer for a mutually acceptable mode. Enter the acceptable modes in your order of preference. Choices for *mode* are: • **gcm-encrypt**—Authentication and encryption **Note** Select this mode for MACsec authentication and encryption if your software license supports MACsec encryption. • **gmac**—Authentication, no encryption • **no-encap**—No encapsulation • **null**—Encapsulation, no authentication or encryption **Note** If the interface is not capable of data link encryption, no-encap is the default and the only available SAP operating mode. SGT is not supported. **Note** Although visible in the CLI help, the timer reauthentication and propagate sgt keywords are not supported.
Step 5	**exit** **Example:** `Switch(config-if-cts-dot1x)# exit`	Exits Cisco TrustSec 802.1x interface configuration mode.
Step 6	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show cts interface** [*interface-id* | **brief** | **summary**]	(Optional) Verify the configuration by displaying TrustSec-related interface characteristics.

	Command or Action	Purpose
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Example

This example shows how to enable Cisco TrustSec authentication in 802.1x mode on an interface using GCM as the preferred SAP mode:

```
Switch# configure terminal
Switch(config)# interface tengigabitethernet 1/1/2
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt null no-encap

Switch(config-if-cts-dot1x)# exit
Switch(config-if)# end
```

Related Topics

Cisco TrustSec Switch-to-Switch Link Security Configuration Example, on page 1082

Configuring Cisco TrustSec Switch-to-Switch Link Security in Manual Mode

Before you begin

When manually configuring Cisco TrustSec on an interface, consider these usage guidelines and restrictions:

- If no SAP parameters are defined, Cisco TrustSec encapsulation or encryption is not performed.
- If you select GCM as the SAP operating mode, you must have a MACsec Encryption software license from Cisco. If you select GCM without the required license, the interface is forced to a link-down state.
- These protection levels are supported when you configure SAP pairwise master key (sap pmk):
  - SAP is not configured—no protection.
  - **sap mode-list gcm-encrypt gmac no-encap**—protection desirable but not mandatory.
  - **sap mode-list gcm-encrypt gmac**—confidentiality preferred and integrity required. The protection is selected by the supplicant according to supplicant preference.
  - **sap mode-list gmac**—integrity only.
  - **sap mode-list gcm-encrypt**—confidentiality required.
  - **sap mode-list gmac gcm-encrypt**—integrity required and preferred, confidentiality optional.
- When CTS is configured on an interface and the System MTU is set to a value greater than 9191, the resulting packet size is limited to 9190.

Beginning in privileged EXEC mode, follow these steps to manually configure Cisco TrustSec on an interface to another Cisco TrustSec device:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface tengigabitethernet 1/1/2`	**Note** Enters interface configuration mode.
Step 3	**cts manual** **Example:** `Switch(config-if)# cts manual`	Enters Cisco TrustSec manual configuration mode.
Step 4	**sap pmk** *key* [**mode-list** *mode1* [*mode2* [*mode3* [*mode4*]]]] **Example:** `Switch(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm-encrypt null no-encap`	(Optional) Configures the SAP pairwise master key (PMK) and operation mode. SAP is disabled by default in Cisco TrustSec manual mode. • *key*—A hexadecimal value with an even number of characters and a maximum length of 32 characters. The SAP operation mode options: • **gcm-encrypt**—Authentication and encryption **Note** Select this mode for MACsec authentication and encryption if your software license supports MACsec encryption. • **gmac**—Authentication, no encryption • **no-encap**—No encapsulation • **null**—Encapsulation, no authentication or encryption **Note** If the interface is not capable of data link encryption, **no-encap** is the default and the only available SAP operating mode. SGT is not supported.

	Command or Action	Purpose
Step 5	**no propagate sgt** **Example:** `Switch(config-if-cts-manual)# no propagate sgt`	Use the **no** form of this command when the peer is incapable of processing a SGT. The **no propagate sgt** command prevents the interface from transmitting the SGT to the peer.
Step 6	**exit** **Example:** `Switch(config-if-cts-manual)# exit`	Exits Cisco TrustSec 802.1x interface configuration mode.
Step 7	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 8	**show cts interface** [*interface-id* | **brief** | **summary**]	(Optional) Verify the configuration by displaying TrustSec-related interface characteristics.

Example

This example shows how to configure Cisco TrustSec authentication in manual mode on an interface:

```
Switch# configure terminal
Switch(config)# interface tengigabitethernet 1/1/2
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm-encrypt null no-encap
Switch(config-if-cts-manual)# no propagate sgt
Switch(config-if-cts-manual)# exit
Switch(config-if)# end
```

Related Topics

Cisco TrustSec Switch-to-Switch Link Security Configuration Example, on page 1082

Configuration Examples

Example: Configuring MACsec on an Interface

Configuring MACsec on an Interface

```
Switch(config)# interface GigabitEthernet1/0/25
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport mode access
Switch(config-if)# macsec
Switch(config-if)# authentication event linksec fail action authorize vlan 2
Switch(config-if)# authentication host-mode multi-domain
Switch(config-if)# authentication linksec policy must-secure
Switch(config-if)# authentication port-control auto
```

```
Switch(config-if)# authentication periodic
Switch(config-if)# authentication timer reauthenticate
Switch(config-if)# authentication violation protect
Switch(config-if)# mka policy replay-policy
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
```

```
Switch# show authentication session interface gigabitethernet6/0/36

Interface MAC Address Method Domain Status Fg Session ID
--------------------------------------------------------------------------------
Gi6/0/36 001b.214c.a98c dot1x DATA Auth 020000D4000019440E54D478
Gi6/0/36 001b.0cdb.bdd8 mab  VOICE Auth 020000D400000FB2001687B2


Key to Session Events Blocked Status Flags:

A - Applying Policy (multi-line status for details)
D - Awaiting Deletion
F - Final Removal in progress
I - Awaiting IIF ID allocation
N - Waiting for AAA to come up
P - Pushed Session
R - Removing User Profile (multi-line status for details)
U - Applying User Profile (multi-line status for details)
X - Unknown Blocker

Runnable methods list:
Handle Priority Name
16 5 dot1x
19 10 mab
23 15 webauth
```

```
Switch# show authentication session interface gigabitethernet6/0/36 details


Interface: GigabitEthernet6/0/36
IIF-ID: 0x1062E8000000AB0
MAC Address: 001b.214c.a98c
IPv6 Address: Unknown
IPv4 Address: 16.0.0.21
User-Name: D_MustSecure
Status: Authorized
Domain: DATA
Oper host mode: multi-domain
Oper control dir: both
Session timeout: 200s (local), Remaining: 187s
Timeout action: Reauthenticate
Common Session ID: 020000D4000019440E54D478
Acct Session ID: 0x000019D8
Handle: 0x86000996
Current Policy: POLICY_Gi6/0/36

Local Policies:
Idle timeout: 60 sec
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
Vlan Group: Vlan: 16
```

```
Security Policy: Must Secure
Security Status: Link Secured
SGT Value: 0

Method status list:
Method State
dot1x Authc Success

---------------------------------------
Interface: GigabitEthernet6/0/36
IIF-ID: 0x100200000000120
MAC Address: 001b.0cdb.bdd8
IPv6 Address: Unknown
IPv4 Address: Unknown
User-Name: 00-1B-0C-DB-BD-D8
Status: Authorized
Domain: VOICE
Oper host mode: multi-domain
Oper control dir: both
Session timeout: 200s (local), Remaining: 177s
Timeout action: Reauthenticate
Common Session ID: 020000D400000FB2001687B2
Acct Session ID: 0x000019DB

Handle: 0x0A000006
Current Policy: POLICY_Gi6/0/36

Local Policies:
Idle timeout: 60 sec
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
Vlan Group: Vlan: 116
Security Policy: Must Not Secure
Security Status: Link Unsecure

Method status list:
Method State
dot1x Stopped
mab Authc Success

Switch# show macsec interface gigabitethernet6/0/3615
MACsec is enabled
Replay protect : enabled
Replay window : 0
Include SCI : yes
Use ES Enable : no
Use SCB Enable : no
Admin Pt2Pt MAC : forceTrue(1)
Pt2Pt MAC Operational : no
Cipher : GCM-AES-128
Confidentiality Offset : 0

Capabilities
Identifier :
Name :
ICV length : 16
Data length change supported: yes
Max. Rx SA : 16
Max. Tx SA : 16
Max. Rx SC : 8
Max. Tx SC : 8
Validate Frames : strict
PN threshold notification support : Yes
```

```
Ciphers supported : GCM-AES-128

Transmit Secure Channels
SCI : B000B43A70A40002
SC state : notInUse(2)
Elapsed time : 00:05:25
Start time : 7w0d
Current AN: 1
Previous AN: 0
Next PN: 0
SA State: notInUse(2)
Confidentiality : no
SAK Unchanged : no
SA Create time : 2d18h
SA Start time : 7w0d
SC Statistics
Auth-only Pkts : 0
Auth-only Bytes : 0
Encrypt Pkts : 308
Encrypt Bytes : 0
SA Statistics
Auth-only Pkts : 0
Encrypt Pkts : 182

Port Statistics

Receive Secure Channels
SCI : 001B214CA98C0000
SC state : notInUse(2)
Elapsed time : 00:05:25
Start time : 7w0d
Current AN: 1
Previous AN: 0
Next PN: 0
RX SA Count: 0
SA State: notInUse(2)
SAK Unchanged : no
SA Create time : 2d18h
SA Start time : 7w0d
SC Statistics
Notvalid pkts 0
Invalid pkts 0
Valid pkts 495
Valid bytes 0
Late pkts 0
Uncheck pkts 0
Delay pkts 0
UnusedSA pkts 0
NousingSA pkts 0
Decrypt bytes 0
SA Statistics
Notvalid pkts 0
Invalid pkts 0
Valid pkts 146
UnusedSA pkts 0
NousingSA pkts 0

Port Statistics
#
```

Related Topics

Configuring MACsec on an Interface, on page 1069
Configuring an MKA Policy, on page 1068

Default MACsec MKA Configuration, on page 1067

Cisco TrustSec Switch-to-Switch Link Security Configuration Example

This example shows the configuration necessary for a seed and non-seed device for Cisco TrustSec switch-to-switch security. You must configure the AAA and RADIUS for link security. In this example, ACS-1 through ACS-3 can be any server names and cts-radius is the Cisco TrustSec server.

Seed Device Configuration:

```
Switch(config)# aaa new-model
Switch(config)# radius server ACS-1
Switch(config-radius-server)# address ipv4 10.5.120.12 auth-port 1812 acct-port
 1813
Switch(config-radius-server)# pac key cisco123
Switch(config-radius-server)# exit
Switch(config)# radius server ACS-2
Switch(config-radius-server)# address ipv4 10.5.120.14 auth-port 1812 acct-port
 1813
Switch(config-radius-server)# pac key cisco123
Switch(config-radius-server)# exit
Switch(config)# radius server ACS-3
Switch(config-radius-server)# address ipv4 10.5.120.15 auth-port 1812 acct-port
 1813
Switch(config-radius-server)# pac key cisco123
Switch(config-radius-server)# exit
Switch(config)# aaa group server radius cts-radius
Switch(config-sg-radius)# server name ACS-1
Switch(config-sg-radius)# server name ACS-2
Switch(config-sg-radius)# server name ACS-3
Switch(config-sg-radius)# exit
Switch(config)# aaa authentication login default none
Switch(config)# aaa authentication dot1x default group cts-radius
Switch(config)# aaa authorization network cts-radius group cts-radius
Switch(config)# aaa session-id common
Switch(config)# cts authorization list cts-radius
Switch(config)# dot1x system-auth-control

Switch(config)# interface gi1/1/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt gmac

Switch(config-if-cts-dot1x)# exit
Switch(config-if)# exit

Switch(config)# interface gi1/1/4
Switch(config-if)# switchport mode trunk
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk 033445AABBCCDDEEFF mode-list gcm-encrypt
 gmac
Switch(config-if-cts-manual)# no propagate sgt
```

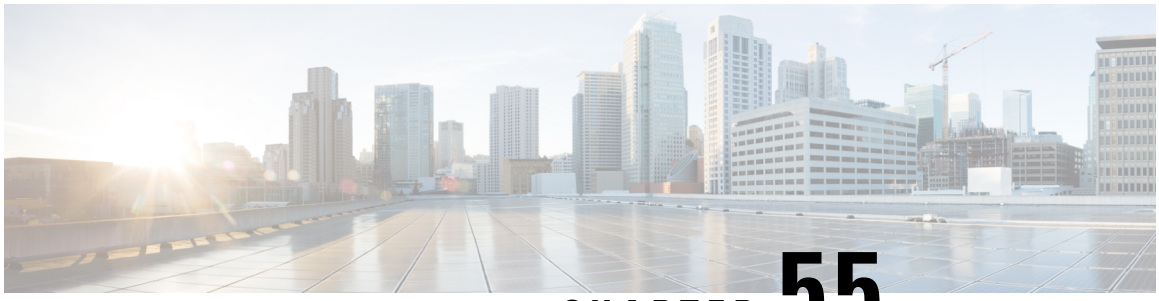
```
Switch(config-if-cts-manual)# exit
Switch(config-if)# exit

Switch(config)# radius-server vsa send authentication
Switch(config)# exit
Switch# cts credentials id cts-36 password trustsec123
```

Non-Seed Device:

```
Switch(config)# aaa new-model
Switch(config)# aaa session-id common
Switch(config)# dot1x system-auth-control

Switch(config)# interface gi1/1/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# shutdown
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)#sap mode-list gcm-encrypt gmac
Switch(config-if-cts-dot1x)#exit
Switch(config-if)#exit

Switch(config)# interface gi1/1/4
Switch(config-if)# switchport mode trunk
Switch(config-if)# shutdown
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk 033445AABBCCDDEEFF mode-list gcm-encrypt
 gmac
Switch(config-if-cts-manual)# no propagate sgt
Switch(config-if-cts-manual)# exit
Switch(config-if)# exit

Switch(config)# radius-server vsa send authentication
Switch(config)# end
Switch# cts credentials id cts-72 password trustsec123
```

Related Topics

Configuring Cisco TrustSec Switch-to-Switch Link Security in 802.1x Mode, on page 1074
Configuring Cisco TrustSec Switch-to-Switch Link Security in Manual Mode, on page 1076



CHAPTER 55

Configuring Web-Based Authentication

This chapter describes how to configure web-based authentication on the switch. It contains these sections:

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Web-Based Authentication Overview

Use the web-based authentication feature, known as web authentication proxy, to authenticate end users on host systems that do not run the IEEE 802.1x supplicant.

Note You can configure web-based authentication on Layer 2 and Layer 3 interfaces.

When you initiate an HTTP session, web-based authentication intercepts ingress HTTP packets from the host and sends an HTML login page to the users. The users enter their credentials, which the web-based authentication feature sends to the authentication, authorization, and accounting (AAA) server for authentication.

If authentication succeeds, web-based authentication sends a Login-Successful HTML page to the host and applies the access policies returned by the AAA server.

If authentication fails, web-based authentication forwards a Login-Fail HTML page to the user, prompting the user to retry the login. If the user exceeds the maximum number of attempts, web-based authentication forwards a Login-Expired HTML page to the host, and the user is placed on a watch list for a waiting period.

Note HTTPS traffic interception for central web authentication redirect is not supported.

Note You should use global parameter-map (for method-type, custom, and redirect) only for using the same web authentication methods like consent, web consent, and webauth, for all the clients and SSIDs. This ensures that all the clients have the same web-authentication method.

If the requirement is to use Consent for one SSID and Web-authentication for another SSID, then you should use two named parameter-maps. You should configure Consent in first parameter-map and configure webauth in second parameter-map.

Note The traceback that you receive when webauth client tries to do authentication does not have any performance or behavioral impact. It happens rarely when the context for which FFM replied back to EPM for ACL application is already dequeued (possibly due to timer expiry) and the session becomes ‘unauthorized’.

Based on where the web pages are hosted, the local web authention can be categorozied as follows:

- *Internal*—The internal default HTML pages (Login, Success, Fail, and Expire) in the controller are used during the local web authentication.
- *Customized*—The customized web pages (Login, Success, Fail, and Expire) are downloaded onto the controller and used during the local web authentication.
- *External*—The customized web pages are hosted on the external web server instead of using the in-built or custom web pages.

Based on the various web authentication pages, the types of web authentication are as follows:

- *Webauth*—This is a basic web authentication. Herein, the controller presents a policy page with the user name and password. You need to enter the correct credentials to access the network.
- *Consent or web-passthrough*—Herein, the controller presents a policy page with the Accept or Deny buttons. You need to click the Accept button to access the network.
- *Webconsent*—This is a combination of webauth and consent web authentication types. Herein, the controller presents a policy page with Accept or Deny buttons along with user name or password. You need to enter the correct credentials and click the Accept button to access the network.

Note The Wireless web authentication feature does not support the bypass type.

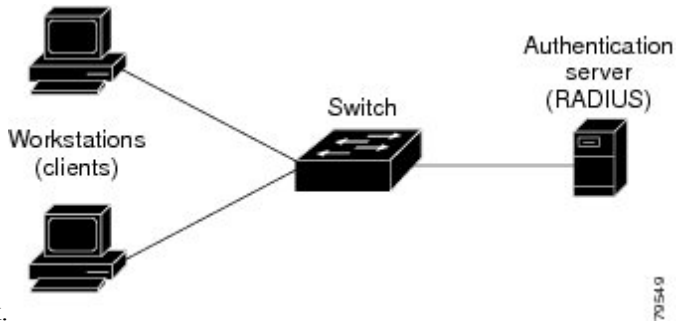
Device Roles

With web-based authentication, the devices in the network have these specific roles:

- *Client*—The device (workstation) that requests access to the LAN and the services and responds to requests from the switch. The workstation must be running an HTML browser with Java Script enabled.
- *Authentication server*—Authenticates the client. The authentication server validates the identity of the client and notifies the switch that the client is authorized to access the LAN and the switch services or that the client is denied.
- *Switch*—Controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client.

Figure 64: Web-Based Authentication Device Roles

This figure shows the roles of these devices in a network.



Host Detection

The switch maintains an IP device tracking table to store information about detected hosts.

Note By default, the IP device tracking feature is disabled on a switch. You must enable the IP device tracking feature to use web-based authentication.

For Layer 2 interfaces, web-based authentication detects IP hosts by using these mechanisms:

- ARP based trigger—ARP redirect ACL allows web-based authentication to detect hosts with a static IP address or a dynamic IP address.
- Dynamic ARP inspection
- DHCP snooping—Web-based authentication is notified when the switch creates a DHCP-binding entry for the host.

Session Creation

When web-based authentication detects a new host, it creates a session as follows:

- Reviews the exception list.

  If the host IP is included in the exception list, the policy from the exception list entry is applied, and the session is established.

- Reviews for authorization bypass

  If the host IP is not on the exception list, web-based authentication sends a nonresponsive-host (NRH) request to the server.

  If the server response is access accepted, authorization is bypassed for this host. The session is established.

- Sets up the HTTP intercept ACL

  If the server response to the NRH request is access rejected, the HTTP intercept ACL is activated, and the session waits for HTTP traffic from the host.

Authentication Process

When you enable web-based authentication, these events occur:

- The user initiates an HTTP session.
- The HTTP traffic is intercepted, and authorization is initiated. The switch sends the login page to the user. The user enters a username and password, and the switch sends the entries to the authentication server.
- If the authentication succeeds, the switch downloads and activates the user's access policy from the authentication server. The login success page is sent to the user.
- If the authentication fails, the switch sends the login fail page. The user retries the login. If the maximum number of attempts fails, the switch sends the login expired page, and the host is placed in a watch list. After the watch list times out, the user can retry the authentication process.
- If the authentication server does not respond to the switch, and if an AAA fail policy is configured, the switch applies the failure access policy to the host. The login success page is sent to the user.
- The switch reauthenticates a client when the host does not respond to an ARP probe on a Layer 2 interface, or when the host does not send any traffic within the idle timeout on a Layer 3 interface.
- The feature applies the downloaded timeout or the locally configured session timeout.

  Note Beginning with Cisco IOS XE Denali 16.1.1 and later, the default session timeout value for web-based authentication on WLC is 1800 seconds. The default session timeout value was infinite seconds, prior to Cisco IOS XE Denali 16.1.1.

- If the terminate action is RADIUS, the feature sends a nonresponsive host (NRH) request to the server. The terminate action is included in the response from the server.
- If the terminate action is default, the session is dismantled, and the applied policy is removed.

Local Web Authentication Banner

With Web Authentication, you can create a default and customized web-browser banners that appears when you log in to a switch.

The banner appears on both the login page and the authentication-result pop-up pages. The default banner messages are as follows:

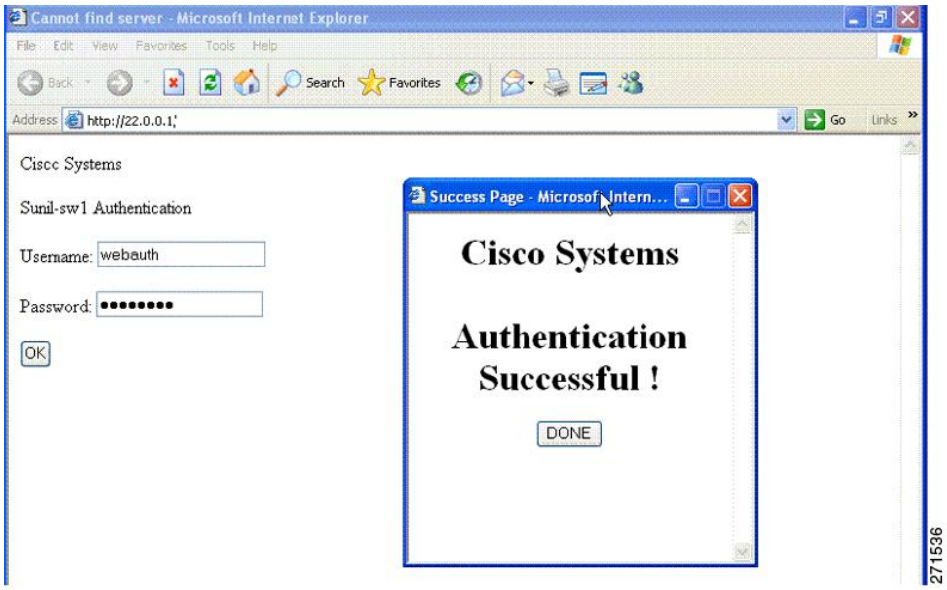
- *Authentication Successful*
- *Authentication Failed*
- *Authentication Expired*

The Local Web Authentication Banner can be configured in legacy CLIs as follows:

- Legacy mode—Use the **ip admission auth-proxy-banner http** global configuration command.
- New-style mode—Use the **parameter-map type webauth global banner** global configuration command.

The default banner *Cisco Systems* and *Switch host-name Authentication* appear on the Login Page. *Cisco Systems* appears on the authentication result pop-up page.

Figure 65: Authentication Successful Banner

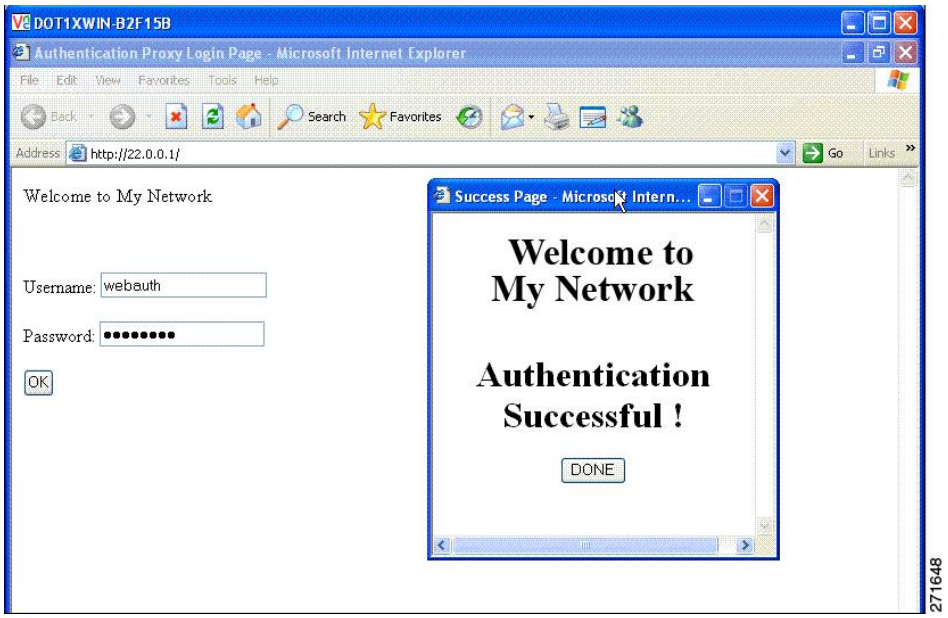


The banner can be customized as follows:

- Add a message, such as switch, router, or company name to the banner:
  - Legacy mode—Use the **ip admission auth-proxy-banner http** *banner-text*global configuration command.
  - New-style mode—Use the **parameter-map type webauth global banner** global configuration command.
- Add a logo or text file to the banner:

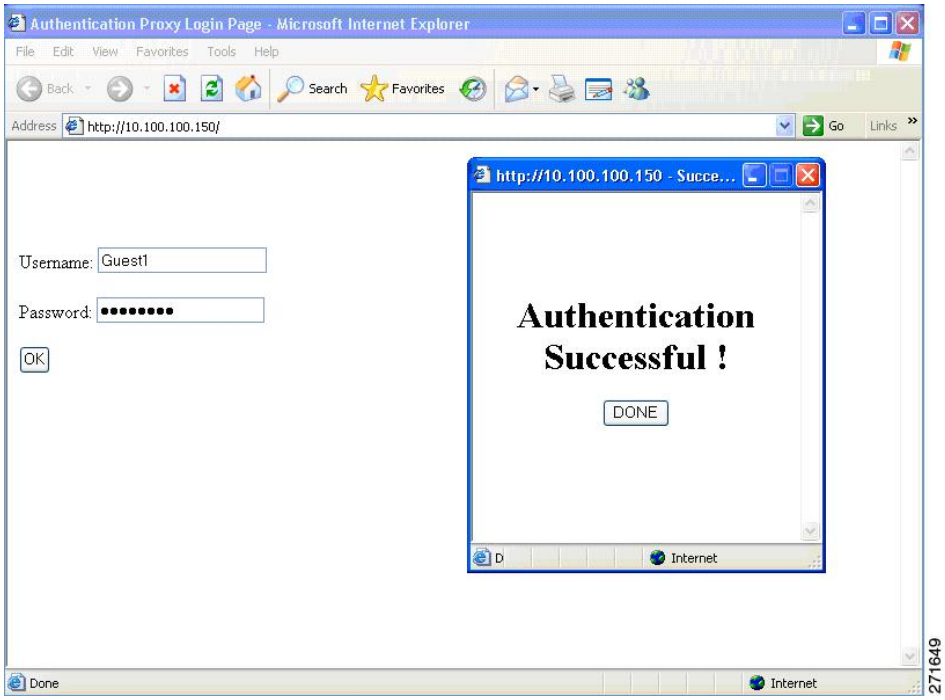
- Legacy mode—Use the **ip admission auth-proxy-banner http** *file-path* global configuration command.
- New-style mode—Use the **parameter-map type webauth global banner** global configuration command.

Figure 66: Customized Web Banner



If you do not enable a banner, only the username and password dialog boxes appear in the web authentication login screen, and no banner appears when you log into the switch.

Figure 67: Login Screen With No Banner



For more information, see the *Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)* and the *Web Authentication Enhancements - Customizing Authentication Proxy Web Pages*.

Web Authentication Customizable Web Pages

During the web-based authentication process, the switch internal HTTP server hosts four HTML pages to deliver to an authenticating client. The server uses these pages to notify you of these four-authentication process states:

- Login—Your credentials are requested.
- Success—The login was successful.
- Fail—The login failed.
- Expire—The login session has expired because of excessive login failures.

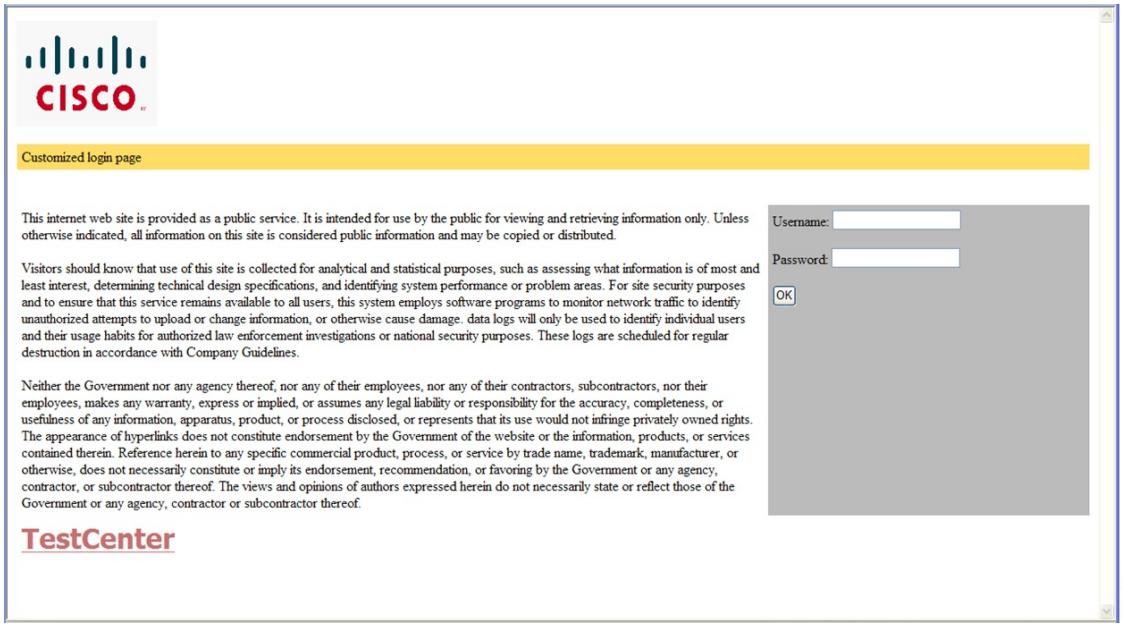
Guidelines

- You can substitute your own HTML pages for the default internal HTML pages.
- You can use a logo or specify text in the *login*, *success*, *failure*, and *expire* web pages.
- On the banner page, you can specify text in the login page.
- The pages are in HTML.
- You must include an HTML redirect command in the success page to access a specific URL.

- The URL string must be a valid URL (for example, http://www.cisco.com). An incomplete URL might cause *page not found* or similar errors on a web browser.
- If you configure web pages for HTTP authentication, they must include the appropriate HTML commands (for example, to set the page time out, to set a hidden password, or to confirm that the same page is not submitted twice).
- The CLI command to redirect users to a specific URL is not available when the configured login form is enabled. The administrator should ensure that the redirection is configured in the web page.
- If the CLI command redirecting users to specific URL after authentication occurs is entered and then the command configuring web pages is entered, the CLI command redirecting users to a specific URL does not take effect.
- Configured web pages can be copied to the switch boot flash or flash.
- On stackable switches, configured pages can be accessed from the flash on the stack master or members.
- The login page can be on one flash, and the success and failure pages can be another flash (for example, the flash on the stack master or a member).
- You must configure all four pages.
- The banner page has no effect if it is configured with the web page.
- All of the logo files (image, flash, audio, video, and so on) that are stored in the system directory (for example, flash, disk0, or disk) and that must be displayed on the login page must use *web_auth_<filename>* as the file name.
- The configured authentication proxy feature supports both HTTP and SSL.

You can substitute your HTML pages for the default internal HTML pages. You can also specify a URL to which users are redirected after authentication occurs, which replaces the internal Success page.

Figure 68: Customizable Authentication Page



Authentication Proxy Web Page Guidelines

When configuring customized authentication proxy web pages, follow these guidelines:

- To enable the custom web pages feature, specify all four custom HTML files. If you specify fewer than four files, the internal default HTML pages are used.
- The four custom HTML files must be present on the flash memory of the switch. The maximum size of each HTML file is 8 KB.
- Any images on the custom pages must be on an accessible HTTP server. Configure an intercept ACL within the admission rule.
- Any external link from a custom page requires configuration of an intercept ACL within the admission rule.
- To access a valid DNS server, any name resolution required for external links or images requires configuration of an intercept ACL within the admission rule.
- If the custom web pages feature is enabled, a configured auth-proxy-banner is not used.
- If the custom web pages feature is enabled, the redirection URL for successful login feature is not available.
- To remove the specification of a custom file, use the **no** form of the command.

Because the custom login page is a public web form, consider these guidelines for the page:

- The login form must accept user entries for the username and password and must show them as **uname** and **pwd**.
- The custom login page should follow best practices for a web form, such as page timeout, hidden password, and prevention of redundant submissions.

Related Topics

Customizing the Authentication Proxy Web Pages, on page 1103

Redirection URL for Successful Login Guidelines

When configuring a redirection URL for successful login, consider these guidelines:

- If the custom authentication proxy web pages feature is enabled, the redirection URL feature is disabled and is not available in the CLI. You can perform redirection in the custom-login success page.
- If the redirection URL feature is enabled, a configured auth-proxy-banner is not used
- To remove the specification of a redirection URL, use the **no** form of the command.
- If the redirection URL is required after the web-based authentication client is successfully authenticated, then the URL string must start with a valid URL (for example, http://) followed by the URL information. If only the URL is given without http://, then the redirection URL on successful authentication might cause page not found or similar errors on a web browser.

Related Topics

Specifying a Redirection URL for Successful Login, on page 1104

Custom Web Authentication Guidelines

- You cannot specify a directory path of a file when downloading a tar bundle from the controller GUI. The tar file is stored in the default flash path.
- You can provide any image name for web authentication and the image name need not be **webauth**.

Web-based Authentication Interactions with Other Features

Port Security

You can configure web-based authentication and port security on the same port. Web-based authentication authenticates the port, and port security manages network access for all MAC addresses, including that of the client. You can then limit the number or group of clients that can access the network through the port.

Related Topics

Enabling and Configuring Port Security

LAN Port IP

You can configure LAN port IP (LPIP) and Layer 2 web-based authentication on the same port. The host is authenticated by using web-based authentication first, followed by LPIP posture validation. The LPIP host policy overrides the web-based authentication host policy.

If the web-based authentication idle timer expires, the NAC policy is removed. The host is authenticated, and posture is validated again.

Gateway IP

You cannot configure Gateway IP (GWIP) on a Layer 3 VLAN interface if web-based authentication is configured on any of the switch ports in the VLAN.

You can configure web-based authentication on the same Layer 3 interface as Gateway IP. The host policies for both features are applied in software. The GWIP policy overrides the web-based authentication host policy.

ACLs

If you configure a VLAN ACL or a Cisco IOS ACL on an interface, the ACL is applied to the host traffic only after the web-based authentication host policy is applied.

For Layer 2 web-based authentication, it is more secure, though not required, to configure a port ACL (PACL) as the default access policy for ingress traffic from hosts connected to the port. After authentication, the web-based authentication host policy overrides the PACL. The Policy ACL is applied to the session even if there is no ACL configured on the port.

You cannot configure a MAC ACL and web-based authentication on the same interface.

You cannot configure web-based authentication on a port whose access VLAN is configured for VACL capture.

Context-Based Access Control

Web-based authentication cannot be configured on a Layer 2 port if context-based access control (CBAC) is configured on the Layer 3 VLAN interface of the port VLAN.

EtherChannel

You can configure web-based authentication on a Layer 2 EtherChannel interface. The web-based authentication configuration applies to all member channels.

How to Configure Web-Based Authentication

Default Web-Based Authentication Configuration

The following table shows the default web-based authentication configuration.

Table 78: Default Web-based Authentication Configuration

Feature	Default Setting
AAA	Disabled
RADIUS server • IP address • UDP authentication port • Key	• None specified • 1645 • None specified
Default value of inactivity timeout	3600 seconds
Inactivity timeout	Enabled

Web-Based Authentication Configuration Guidelines and Restrictions

- Web-based authentication is an ingress-only feature.
- You can configure web-based authentication only on access ports. Web-based authentication is not supported on trunk ports, EtherChannel member ports, or dynamic trunk ports.
- External web authentication, where the switch redirects a client to a particular host or web server for displaying login message, is not supported.
- You cannot authenticate hosts on Layer 2 interfaces with static ARP cache assignment. These hosts are not detected by the web-based authentication feature because they do not send ARP messages.
- By default, the IP device tracking feature is disabled on a switch. You must enable the IP device tracking feature to use web-based authentication.
- You must configure at least one IP address to run the switch HTTP server. You must also configure routes to reach each host IP address. The HTTP server sends the HTTP login page to the host.
- Hosts that are more than one hop away might experience traffic disruption if an STP topology change results in the host traffic arriving on a different port. This occurs because the ARP and DHCP updates might not be sent after a Layer 2 (STP) topology change.

- Web-based authentication does not support VLAN assignment as a downloadable-host policy.
- Web-based authentication supports IPv6 in Session-aware policy mode. IPv6 Web-authentication requires at least one IPv6 address configured on the switch and IPv6 Snooping configured on the switchport.
- Web-based authentication and Network Edge Access Topology (NEAT) are mutually exclusive. You cannot use web-based authentication when NEAT is enabled on an interface, and you cannot use NEAT when web-based authentication is running on an interface.
- Web-based authentication NRH (Non-Responsive Host) is not supported for voice devices.
- Only the Password Authentication Protocol (PAP) is supported for web-based RADIUS authentication on controllers. The Challenge Handshake Authentication Protocol (CHAP) is not supported for web-based RADIUS authentication on controllers.
- Identify the following RADIUS security server settings that will be used while configuring switch-to-RADIUS-server communication:
  - Host name
  - Host IP address
  - Host name and specific UDP port numbers
  - IP address and specific UDP port numbers

  The combination of the IP address and UDP port number creates a unique identifier, that enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service (for example, authentication) the second host entry that is configured functions as the failover backup to the first one. The RADIUS host entries are chosen in the order that they were configured.
- When you configure the RADIUS server parameters:
  - Specify the **key** *string* on a separate command line.
  - For **key** *string*, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server.
  - When you specify the **key** *string*, use spaces within and at the end of the key. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon.
  - You can globally configure the timeout, retransmission, and encryption key values for all RADIUS servers by using with the **radius-server host** global configuration command. If you want to configure these options on a per-server basis, use the **radius-server timeout**, radius-server transmit, and the radius-server key global configuration commands. For more information, see the *Cisco IOS Security Configuration Guide*, Release 12.4 and the *Cisco IOS Security Command Reference*, Release 12.4.

Note You need to configure some settings on the RADIUS server, including: the switch IP address, the key string to be shared by both the server and the switch, and the downloadable ACL (DACL). For more information, see the RADIUS server documentation.

- When you upgrade from IOS XE release 3.6.x and 3.7.x, ensure that you use **radius-server attribute wireless accounting call-station-id macaddress** command to configure mac-address. This is because the accounting default call-station-id is changed from mac-address to IP address from Cisco IOS XE Denali 16.3.x onwards.

Web-Based Authentication Configuration Task List

Configuring the Authentication Rule and Interfaces

Examples in this section are legacy-style configurations. For new-style configurations, see the *Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Follow these steps to configure the authentication rule and interfaces:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip admission name** *name* **proxy http** **Example:** `Switch(config)# ip admission name webauth1 proxy http`	Configures an authentication rule for web-based authorization.
Step 4	**interface** *type slot/port* **Example:** `Switch(config)# interface gigabitEthernet1/0/1`	Enters interface configuration mode and specifies the ingress Layer 2 or Layer 3 interface to be enabled for web-based authentication. *type* can be fastethernet, gigabit ethernet, or tengigabitethernet.
Step 5	**ip access-group** *name* **Example:** `Switch(config-if)# ip access-group webauthag`	Applies the default ACL.

	Command or Action	Purpose
Step 6	**ip admission name** **Example:** `Switch(config)# ip admission name`	Configures an authentication rule for web-based authorization for the interface.
Step 7	**exit** **Example:** `Switch(config-if)# exit`	Returns to configuration mode.
Step 8	**ip device tracking** **Example:** `Switch(config)# ip device tracking`	Enables the IP device tracking table.
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 10	**show ip admission status** **Example:** `Switch# show ip admission status`	Displays the configuration.
Step 11	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring AAA Authentication

If a method-list is configured under VTY lines, the corresponding method list must be added to the AAA configuration:

```
line vty 0 4
 authorization commands 15 abc
aaa authorization commands 15 abc group tacacs+
```

If a method-list is not configured under VTY lines, you must add the default method list to the AAA configuration:

```
line vty 0 4
 aaa authorization commands 15 default group tacacs+
```

Follow these steps to configure AAA authentication:

Note Use default list for AAA authorization, if you are planning to use features such as dACL.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables AAA functionality.
Step 4	**aaa authentication login default group** {**tacacs+** | **radius**} **Example:** `Switch(config)# aaa authentication login default group tacacs+`	Defines the list of authentication methods at login. **named_authentication_list** refers to any name that is not greater than 31 characters. **AAA_group_name** refers to the server group name. You need to define the server-group **server_name** at the beginning itself.
Step 5	**aaa authorization auth-proxy default group** {**tacacs+** | **radius**} **Example:** `Switch(config)# aaa authorization auth-proxy default group tacacs+`	Creates an authorization method list for web-based authorization.
Step 6	**tacacs server** *server-name* **Example:**	Specifies an AAA server.

	Command or Action	Purpose
	`Switch(config)# tacacs server yourserver`	
Step 7	**address** {**ipv4** | **ipv6**} *ip address* **Example:** `Switch(config-server-tacacs)# address ipv4 10.0.1.12`	Configures the IP address for the TACACS server.
Step 8	**key** *string* **Example:** `Switch(config-server-tacacs)# key cisco123`	Configures the authorization and encryption key used between the switch and the TACACS server.
Step 9	**exit** **Example:** `Switch(config-server-tacacs)# exit`	Exits the TACACS server mode and enters the global configuration mode.
Step 10	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 11	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 12	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Switch-to-RADIUS-Server Communication

Follow these steps to configure the RADIUS server parameters:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip radius source-interface vlan** *vlan interface number* **Example:** `Switch(config)# ip radius source-interface vlan 80`	Specifies that the RADIUS packets have the IP address of the indicated interface.
Step 4	**radius server** *server name* **Example:** `Switch(config)# radius server rsim address ipv4 124.2.2.12`	(Optional) Specifies the IP address of the RADIUS server.
Step 5	**address** {**ipv4** | **ipv6**} *ip address* **Example:** `Switch(config-radius-server)# address ipv4 10.0.1.2 auth-port 1550 acct-port 1560`	Configures the IP address for the RADIUS server.
Step 6	**key** *string* **Example:** `Switch(config-radius-server)# key rad123`	(Optional) Specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.
Step 7	**exit** **Example:** `Switch(config-radius-server)# exit`	Exits the RADIUS server mode and enters the global configuration mode.

	Command or Action	Purpose
Step 8	**radius-server dead-criteria tries** *num-tries* **Example:** `Switch(config)# radius-server dead-criteria tries 30`	Specifies the number of unanswered sent messages to a RADIUS server before considering the server to be inactive. The range of *num-tries* is 1 to 100.
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Configuring the HTTP Server

To use web-based authentication, you must enable the HTTP server within the Switch. You can enable the server for either HTTP or HTTPS.

Note The Apple psuedo-browser will not open if you configure only the **ip http secure-server** command. You should also configure the **ip http server** command.

Follow these steps to enable the server for either HTTP or HTTPS:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip http server** **Example:** `Switch(config)# ip http server`	Enables the HTTP server. The web-based authentication feature uses the HTTP server to communicate with the hosts for user authentication.
Step 4	**ip http secure-server**	Enables HTTPS.

	Command or Action	Purpose
	Example: `Switch(config)# ip http secure-server`	You can configure custom authentication proxy web pages or specify a redirection URL for successful login. **Note** To ensure secure authentication when you enter the **ip http secure-server** command, the login page is always in HTTPS (secure HTTP) even if the user sends an HTTP request.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Customizing the Authentication Proxy Web Pages

You can configure web authentication to display four substitute HTML pages to the user in place of the Switch default HTML pages during web-based authentication.

For the equivalent Session Aware Networking configuration example for this feature, see the section "Configuring a Parameter Map for Web-Based Authentication" in the chapter, "Configuring Identity Control Policies." of the book, "*Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*."

Follow these steps to specify the use of your custom authentication proxy web pages:

Before you begin

Store your custom HTML files on the Switch flash memory.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip admission proxy http login page file** *device:login-filename*	Specifies the location in the Switch memory file system of the custom HTML file to use in

	Command or Action	Purpose
	Example: `Switch(config)# ip admission proxy http login page file disk1:login.htm`	place of the default login page. The *device:* is flash memory.
Step 4	**ip admission proxy http success page file** *device:success-filename* **Example:** `Switch(config)# ip admission proxy http success page file disk1:success.htm`	Specifies the location of the custom HTML file to use in place of the default login success page.
Step 5	**ip admission proxy http failure page file** *device:fail-filename* **Example:** `Switch(config)# ip admission proxy http fail page file disk1:fail.htm`	Specifies the location of the custom HTML file to use in place of the default login failure page.
Step 6	**ip admission proxy http login expired page file** *device:expired-filename* **Example:** `Switch(config)# ip admission proxy http login expired page file disk1:expired.htm`	Specifies the location of the custom HTML file to use in place of the default login expired page.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Related Topics

Authentication Proxy Web Page Guidelines, on page 1093

Specifying a Redirection URL for Successful Login

Follow these steps to specify a URL to which the user is redirected after authentication, effectively replacing the internal Success HTML page:

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Switch> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip admission proxy http success redirect** *url-string* **Example:** `Switch(config)# ip admission proxy http success redirect www.example.com`	Specifies a URL for redirection of the user in place of the default login success page.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Related Topics

Redirection URL for Successful Login Guidelines, on page 1093

Configuring the Web-Based Authentication Parameters

Follow these steps to configure the maximum number of failed login attempts before the client is placed in a watch list for a waiting period:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose
Step 3	**ip admission max-login-attempts** *number* **Example:** `Switch(config)# ip admission max-login-attempts 10`	Sets the maximum number of failed login attempts. The range is 1 to 2147483647 attempts. The default is 5.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring a Web-Based Authentication Local Banner

Follow these steps to configure a local banner on a switch that has web authentication configured.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip admission auth-proxy-banner http** [*banner-text* | *file-path*]	Enables the local banner.

	Command or Action	Purpose
	Example: `Switch(config)# ip admission auth-proxy-banner http C My Switch C`	(Optional) Create a custom banner by entering *C banner-text C* (where *C* is a delimiting character), or *file-path* that indicates a file (for example, a logo or text file) that appears in the banner.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Web-Based Authentication without SVI

You configure the web-based authentication without SVI feature to redirect the HTML login page to the client without creating an IP address in the routing table. These steps are optional.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**parameter-map type webauth global** **Example:**	Creates a parameter map and enters parameter-map webauth configuration mode. The specific configuration commands supported

	Command or Action	Purpose
	`Switch (config)# parameter-map type webauth global`	for a global parameter map defined with the global keyword differ from the commands supported for a named parameter map defined with the parameter-map-name argument.
Step 4	**l2-webauth-enabled** **Example:** `Switch (config-params-parameter-map)# l2-webauth-enabled`	Enables the web-based authentication without SVI feature
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Web-Based Authentication with VRF Aware

You configure the web-based authentication with VRF aware to redirect the HTML login page to the client. These steps are optional.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose
Step 3	**parameter-map type webauth global** **Example:** `Switch (config)# parameter-map type webauth global`	Creates a parameter map and enters parameter-map webauth configuration mode. The specific configuration commands supported for a global parameter map defined with the global keyword differ from the commands supported for a named parameter map defined with the parameter-map-name argument.
Step 4	**webauth-vrf-aware** **Example:** `Switch (config-params-parameter-map)# webauth-vrf-aware`	Enables the web-based authentication VRF aware feature on SVI.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Removing Web-Based Authentication Cache Entries

Follow these steps to remove web-based authentication cache entries:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ip auth-proxy cache** {* | *host ip address*} **Example:**	Delete authentication proxy entries. Use an asterisk to delete all cache entries. Enter a

	Command or Action	Purpose
	`Switch# clear ip auth-proxy cache 192.168.4.5`	specific IP address to delete the entry for a single host.
Step 3	**clear ip admission cache** {*| *host ip address*} **Example:** `Switch# clear ip admission cache 192.168.4.5`	Delete authentication proxy entries. Use an asterisk to delete all cache entries. Enter a specific IP address to delete the entry for a single host.

Downloading Web Authentication Tar Bundle (CLI)

You can download a tar bundle (.tar) containing all personalized files from the FTP or TFTP server.

Procedure

	Command or Action	Purpose
Step 1	**archive tar /xtract <transfer mode> ://<IP> /<location>/<login filename> < DIRECTORY>** **Example:** `Switch# archive tar /xtract tftp://9.1.0.100/user1/login.tar flash2` `Switch# show flash:` `59 4096 Jan 08 2014 13:19:33.0000000000 +00:00 flash` `60 2574 Jan 08 2014 13:19:51.0000000000 +00:00 flash2/aup.html` `61 4082 Jan 08 2014 13:19:51.0000000000 +00:00 flash2/login.html` `62 70123 Jan 08 2014 13:19:52.0000000000 +00:00 flash2/yourlogo.jpg` `63 344 Jan 08 2014 13:19:51.0000000000 +00:00 flash2/failed.html` `64 1653 Jan 08 2014 13:19:52.0000000000 +00:00 flash2/logout.html` `64 1653 Jan 08 2014 13:19:52.0000000000 +00:00 flash2/expired.html`	Specifies to download a tar bundle (.tar) from the FTP or TFTP server.
Step 2	**archive tar /xtract <transfer mode> ://<IP> /<location>/<login filename> < DIRECTORY> flash-1:** **Example:**	Specifies to download a tar bundle (.tar) from the FTP or TFTP server in high availability environment.

	Command or Action	Purpose
	Switch# archive tar /xtract tftp://10.20.10.10/asd/login.tar abc flash-1: Switch# show flash-1: 29 4096 Jan 09 2014 17:08:49.0000000000 +00:00 30 2574 Jan 09 2014 17:08:49.0000000000 +00:00 aup.html 31 344 Jan 09 2014 17:08:49.0000000000 +00:00 abc/failed.html 32 4082 Jan 09 2014 17:08:49.0000000000 +00:00 alogin.html 33 1653 Jan 09 2014 17:08:49.0000000000 +00:00 logout.html 34 70123 Jan 09 2014 17:08:49.0000000000 +00:00 yourlogo.jpg	

Downloading Web Authentication Tar Bundle (GUI)

Procedure

Step 1 Choose **Configuration** > **Commands** > **Download File** to open the Download File to Controller page.

Step 2 From the **File Type** drop-down list, choose Webauth Bundle.

Step 3 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**

Step 4 In the**IP Address** text box, enter the IP address of the server.

Step 5 In the**File Path** text box, enter the directory path of the software.

Step 6 In the**File Name** text box, enter the name of the controller software file (**filename.aes**).

Integrating Customized Web Authentication Pages into a Parameter Map (CLI)

You can configure the personalized pages into a parameter map. Using the parameter map, you can configure all the personalized pages in one shot. This minimizes the need of configuring all the four custom pages separately. Even if you want to configure only some pages, the others pages use the defaults.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** Switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**parameter-map type webauth** *name* **type** *webauth* **Example:** `Switch(config)# parameter-map type webauth WEB type webauth`	Creates a parameter map.
Step 3	**custom-page login device flash:flash2/login.html** **Example:** `Switch(config-params-parameter-map)# custom-page login device flash:flash2/login.html`	Configures the personalized pages into a parameter map.
Step 4	**custom-page success device flash: flash2/logout.html** **Example:** `Switch(config-params-parameter-map)# custom-page success device flash: flash2/logout.html`	Configures the personalized pages into a parameter map.
Step 5	**custom-page failure device flash: flash2/failed.html** **Example:** `Switch(config-params-parameter-map)# custom-page failure device flash: flash2/failed.html`	Configures the personalized pages into a parameter map.
Step 6	**custom-page login expired device flash: flash2/expired.html** **Example:** `Switch(config-params-parameter-map)# custom-page login expired device flash: flash2/expired.html`	Configures the personalized pages into a parameter map.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Step 8	**show parameter-map type webauth name** *name*
	Example:
	`Switch# show parameter-map type webauth name WEB`
	`Parameter Map Name : WEB`
	`Type :`
	`webauth`
	`Custom Page:`
	`Auth-proxy login : flash:`
	`flash2/login.html`
		Configures the personalized pages into a parameter map.

	Command or Action	Purpose
	Auth-proxy Init State time : 120 sec Auth-proxy Fin Wait time : 3000 milliseconds Webauth max-http connection : 30 Webauth logout-window : Enabled Consent Email : Disabled	

Linking Image in Custom Pages

In custom pages, you can also send back images.

In releases earlier to software release 3E, the custom page had to contain the link to the image as an entire path, in the form of: **<img src="http://<ip-addresss>/flash:web_auth_image.jpg" alt="name">**. The IP address is the management IP address of the controller.

Procedure

	Command or Action	Purpose
Step 1	**<img src="./flash:web_auth_image.jpg" alt="name”>** **Example:** `Switch# <img src="./flash:web_auth_image.jpg" alt="name”>`	Specifies to link image to the custom page. The virtual IP address is automatically used as a source. The logical link implies that you define the virtual IP address in the global parameter map. **Note** You can still define the image full path (with controller IP address). In such case, the IP address is either the management IP or the virtual IP (if configured).

Step 2	**<img src="./flash:web_auth_image.jpg" alt="name”>**
	Example:
	`Switch# show run | sec parameter-map`
	`parameter-map type webauth global`
	` virtual-ip ipv4 192.0.2.1`
	`Sample Webauth_login HTML`
		Specifies to link image to the custom page. The virtual IP address is automatically used as a source. The logical link implies that you define the virtual IP address in the global parameter map.
		Note You can still define the image full path (with controller IP address). In such case, the IP address is either the management IP or the virtual IP (if configured).

Sample Web Authentication Login HTML

You can use the sample web authentication login page (**webauth_login**). If you want to modify or customize the sample page, you need to involve a developer who knows HTML, which is not covered by the Cisco Technical Assistance Center.

```
<HTML><HEAD>
<TITLE>Authentication Proxy Login Page</TITLE>
<script type="text/javascript">
var pxypromptwindow1;
var pxysubmitted = false;
function submitreload() {
    if (pxysubmitted == false) {
        pxypromptwindow1=window.open('', 'pxywindow1', 'resizable=no,width=350,
         height=350,scrollbars=yes');
        pxysubmitted = true;
        return true;
    } else {
        alert("This page can not be submitted twice.");
        return false;
    }
}
</script>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<style type="text/css">
body {
    background-color: #ffffff;
}
</style>
</HEAD>
<BODY>
<H1><img src="http://192.168.2.91/flash:web_auth_logo.png" width="75" height="50"
alt="Cisco Logo" longdesc="http://www.cisco.com"></H1>
<center>
<H2> Wireless Guest Access Web Authentication</H2>
<center>
<iframe src="http://192.168.2.91/flash:web_auth_aup.html" width="950" height="250"
scrolling="auto"></iframe><BR><BR>

<FORM method=post action="/" target="pxywindow1">
  Username: <input type=text name=uname><BR><BR>
  Password: <input type=password name=pwd><BR><BR>
  <input type=submit name=ok value=OK   onClick="return submitreload();">
</FORM><noscript>
<BR>
<UL>
  <H2><FONT COLOR="red">Warning!</FONT></H2>
  <p>JavaScript should be enabled in your Web browser
     for secure authentication</p>
  <LI>Follow the instructions of your Web browser to enable
      JavaScript if you would like to have JavaScript enabled
      for secure authentication</LI>
  <BR>OR<BR><BR>
  <LI> Follow these steps if you want to keep JavaScript
       disabled or if your browser does not support JavaScript
    <OL><BR>
      <LI> Close this Web brower window</LI>
      <LI> Click on Reload button of the original browser window</LI>
    </OL></LI>
</UL>
</noscript>
<center>
```

```
<p> </p>
<img src="http://192.168.2.91/flash:web_auth_cisco.png" alt="Cisco Powered" width="215"
height="136" align="middle" longdesc="http://www.cisco.com">
</center>
</BODY></HTML>
```

Configuring a Parameter Map for Local Web Authentication (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth global** **Example:** `Switch(config)# parameter-map type webauth global`	Creates a parameter map and enters parameter-map webauth configuration mode. The specific configuration commands supported for a global parameter map defined with the global keyword differ from the commands supported for a named parameter map defined with the parameter-map-name argument.
Step 3	**virtual-ip ipv4***ip-address* [**virtual-host***fqdn*] **Example:** `Switch(config-params-parameter-map)# virtual-ip ipv4 1.1.1.1 virtual-host host.cisco.com`	Configures the virtual IP address and redirects users to a virtual host. Optionally, you can also configure a fully qualified domain name (FQDN) for the virtual IP, along with the DNS services.
Step 4	**banner** {*file* | *text*} **Example:** `Switch(config-params-parameter-map)# banner`	Displays a banner on the local web-authentication login web page.
Step 5	**custom-page** **Example:** `Switch(config-params-parameter-map)# custom-page`	Specifies the custom page such as login, expired, success, or failure page.
Step 6	**max-http-conns** **Example:** `Switch(config-params-parameter-map)# max-http-conns`	Specifies the maximum number of HTTP connections per clients.
Step 7	**intercept-https-enable** **Example:** `Switch(config-params-parameter-map)# intercept-https-enable`	Specifies to enable intercept of HTTPS traffic.

	Command or Action	Purpose
Step 8	**ratelimit** **Example:** `Switch(config-params-parameter-map)# ratelimit`	Specifies to rate limit on the number of web authentication sessions.
Step 9	**redirect** **Example:** `Switch(config-params-parameter-map)# redirect`	Specifies to redirect the URL.
Step 10	**timeout** **Example:** `Switch(config-params-parameter-map)# timeout`	Specifies to timeout for the initial state of web authentication.
Step 11	**watch-list** **Example:** `Switch(config-params-parameter-map)# watch-list`	Specifies the watch list of web authentication clients.
Step 12	**virtual-ip ipv4** *virtual -IP-address* **Example:** `Switch(config-params-parameter-map)# virtual-ip ipv4 172.16.16.16`	(Optional) Specifies a virtual IP address for web-based authentication clients. This command is supported in the global parameter map only.
Step 13	**exit** **Example:** `Switch(config-params-parameter-map)# exit`	Specifies to exit from **parameter-map params** configuration mode.
Step 14	**no** **Example:** `Switch(config-params-parameter-map)# no`	Specifies to negate a command or set its defaults.
Step 15	**parameter-map type webauth** *name* **type** *webauth test* **Example:** `Switch(config)# parameter-map type webauth user1 type webauth test`	Specifies parameter map user-defined name for local web-based authentication clients. This command is supported in the global parameter map only.
Step 16	**banner** *bannet-text* **Example:** `Switch(config-params-parameter-map)# banner`	(Optional) Displays a banner on the local web-authentication login web page.

	Command or Action	Purpose
Step 17	**consent email** **Example:** `Switch(config-params-parameter-map)# consent email`	(Optional) Requests a user's e-mail address on the local web-authentication login web page. This command is supported in named parameter maps only.
Step 18	**custom-page** **Example:** `Switch(config-params-parameter-map)# custom-page`	Specifies the custom page such as login, expired, success, or failure page.
Step 19	**max-http-conns** **Example:** `Switch(config-params-parameter-map)# max-http-conns`	Specifies the maximum number of HTTP connections per clients.
Step 20	**redirect** **Example:** `Switch(config-params-parameter-map)# redirect`	Specifies to redirect the URL.
Step 21	**timeout** **Example:** `Switch(config-params-parameter-map)# timeout`	Specifies to timeout for the initial state of web authentication.
Step 22	**type** **Example:** `Switch(config-params-parameter-map)# virtual-ip ipv4 172.16.16.16`	(Optional) Specifies the parameter type such as web authentication or consent, or both.
Step 23	**exit** **Example:** `Switch(config-params-parameter-map)# exit`	Specifies to exit from **parameter-map params** configuration mode.
Step 24	**no** **Example:** `Switch(config-params-parameter-map)# no`	Specifies to negate a command or set its defaults.

Monitoring Web-Based Authentication Status

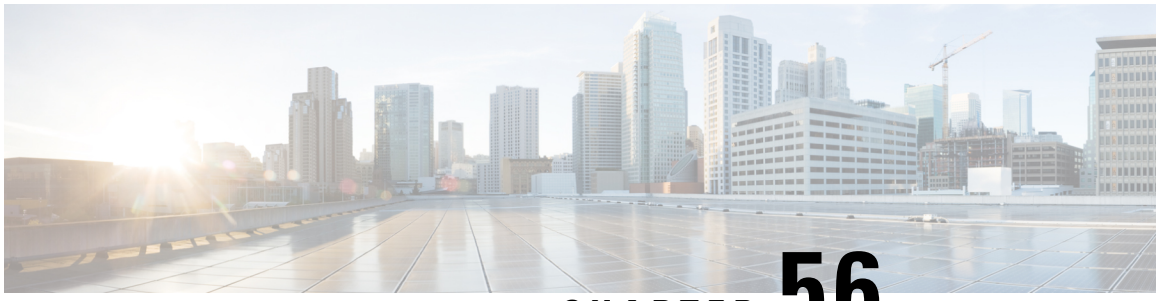
Use the commands in this topic to display the web-based authentication settings for all interfaces or for specific ports.

Table 79: Privileged EXEC show Commands

Command	Purpose
show authentication sessions method webauth	Displays the web-based authentication settings for all interfaces for fastethernet, gigabitethernet, or tengigabitethernet
show wireless client mac-address *a.a.a* **detail**	Displays the session specific wireless information and wireless states.
show authentication sessions interface *type slot/port*[**details**]	Displays the web-based authentication settings for the specified interface for fastethernet, gigabitethernet, or tengigabitethernet. In Session Aware Networking mode, use the **show access-session interface** command.

Feature Information for Web-Based Authentication

Release	Feature Information
Cisco IOS XE 3.2SE	This feature is introduced.



CHAPTER 56

Configuring Cisco TrustSec

Information about Cisco TrustSec

Cisco TrustSec provides security improvements to Cisco network devices based on the capability to strongly identify users, hosts, and network devices within a network. TrustSec provides topology-independent and scalable access controls by uniquely classifying data traffic for a particular role. TrustSec ensures data confidentiality and integrity by establishing trust among authenticated peers and encrypting links with those peers.

The key component of Cisco TrustSec is the Cisco Identity Services Engine (ISE). Cisco ISE can provision switches with TrustSec Identities and Security Group ACLs (SGACLs), though these may be configured manually on the switch.

Finding Feature Information

To configure Cisco Trustsec on the switch, see the Cisco TrustSec Switch Configuration Guide at the following URL:

https://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec.html

Release notes for Cisco TrustSec General Availability releases are at the following URL:

https://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/release/notes/rn_cts_crossplat.html

For restrictions and limitations on Catalyst 3850 and 3650, see the notes available at the following URL:

http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/appa_cat3k.html

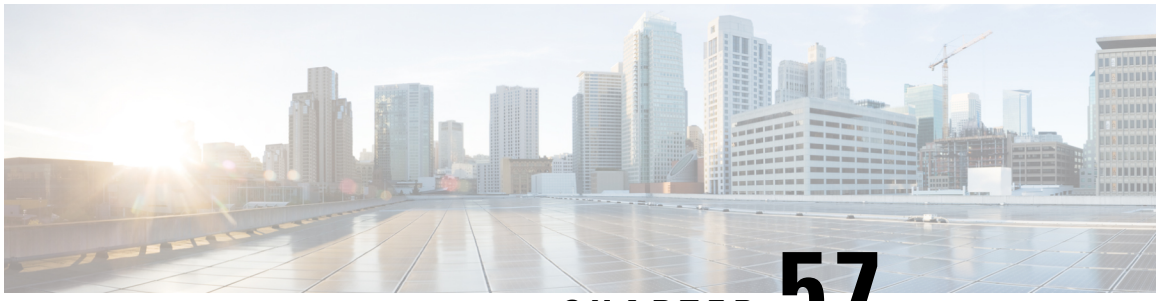
Additional information about the Cisco TrustSec solution, including overviews, datasheets, features by platform matrix, and case studies, is available at the following URL:

https://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html

Feature Information for Cisco TrustSec

Table 80: Feature Information for Cisco TrustSec

Feature Name	Release	Feature Information
• NDAC • SXPv1, SXPv2 • SGT • SGACL Layer2 Enforcement • Interface to SGT and VLAN to SGT mapping. • Subnet to SGT mapping • Layer 3 Port Mapping (PM) • Layer 3 Identity Port Mapping (IPM) • Security Group Name Download • SXP Loop Detection • Policy-based CoA	Cisco IOS XE 3.3SE	These features were introduced on the Catalyst 3850 and 3650 switches.



CHAPTER 57

Configuring Wireless Guest Access

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Guest Access

- All mobility peers should be configured for hierarchical mobility architecture.
- For Guest Controller Mobility Anchor configuration on WLAN is must on Mobility Agent and Guest Controller.
- Guest Access can be a 3 box solution or 2 box solution. The mobility tunnel link status should be up between:
    - Mobility Agent, Mobility Controller and Guest Controller.

  or
    - Mobility Agent/Mobility Controller and Guest Controller

Restrictions for Guess Access

Guest Controller functionality is not supported on the Catalyst 3850 switch whereas Catalyst 3850 can act as mobility agent.

Information about Wireless Guest Access

Ideally, the implementation of a wireless guest network uses as much of an enterprise's existing wireless and wired infrastructure as possible to avoid the cost and complexity of building a physical overlay network. Assuming this is the case, the following additional elements and functions are needed:

- A dedicated guest WLAN/SSID—Implemented throughout the campus wireless network wherever guest access is required. A guest WLAN is identified by a WLAN with mobility anchor (Guest Controller) configured.
- Guest traffic segregation—Requires implementing Layer 2 or Layer 3 techniques across the campus network to restrict where guests are allowed to go.
- Access control—Involves using imbedded access control functionality within the campus network or implementing an external platform to control guest access to the Internet from the enterprise network.
- Guest user credential management—A process by which a sponsor or lobby administrator can create temporary credentials in behalf of a guest. This function might be resident within an access control platform or it might be a component of AAA or some other management system.

Fast Secure Roaming

Fast secure roaming can be achieved by caching the Pairwise Master Key (PMK) information for Cisco Centralized Key Management (CCKM), and 802.11i clients. Cisco Centralized Key Management (CCKM) helps to improve roaming. Only the client can initiate the roaming process, which depends on factors such as:

- Overlap between APs
- Distance between APs
- Channel, signal strength, and load on the AP
- Data rates and output power

Whenever a fast-roaming client 802.11i, [CCKM]) roams to a new device, after fast-roaming the clients go through mobility "handoff" procedure. And new AAA attributes learned through mobility "handoff" procedure get re-applied.

Full L2 authentication must be avoided during roaming if the client uses the 802.11i WPA2, CCKM, to achieve the full requirements of fast secure roaming. The PMK cache (802.11i, CCKM) is used to authenticate and derive the keys for roaming clients to avoid full L2 authentication. This requires all Mobility Anchors (MA) and Mobility Controllers (MC) in the mobility group to have the same PMK cache values.

The session timeout defines when a PMK cache will expire. A PMK cache can also be deleted when a client fails to re-authenticate or when it is manually deleted them from the CLI. The deletion on the original controller or switch shall be propagated to other controllers or switches in the same mobility group.

How to Configure Guest Access

Creating a Lobby Administrator Account

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch # configure terminal`	Enters global configuration mode.
Step 2	**user-name** *user-name* **Example:** `Switch (config)# user-name lobby`	Creates a user account.
Step 3	**type lobby-admin** **Example:** `Switch (config-user-name)# type lobby-admin`	Specifies the account type as lobby admin.
Step 4	**password 0** *password* **Example:** `Switch(config-user-name)# password 0 lobby`	Creates a password for the lobby administrator account.
Step 5	**end** **Example:** `Switch (config-user-name)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config | section** *user-name* (or) **show running-config | section** *configured lobby admin username* **Example:** `Switch # show running-config | section lobby`	Displays the configuration details.

Example

Configuring Guest User Accounts

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch # configure terminal`	Enters global configuration mode.
Step 2	**user-name** *user-name* **Example:** `Switch (config)# user-name guest`	Creates a username for the lobby ambassador account.
Step 3	**password** *unencrypted/hidden-password password* **Example:** `Switch (config-user-name)# password 0 guest`	Specifies the password for the user.
Step 4	**type network-user description** *description* **guest-user lifetime year** *0-1* **month** *0-11* **day** *0-30* **hour** *0-23* **minute** *0-59* **second** *0-59* **Example:** `Switch (config-user-name)# type network-user description guest guest-user lifetime year 1 month 10 day 3 hour 1 minute 5 second 30`	Specifies the type of user.
Step 5	**end** **Example:** `Switch (config-user-name)# end`	Returns to privileged EXEC mode.
Step 6	**show aaa local netuser all** **Example:** `Switch # show aaa local netuser all`	Displays the configuration details. After the lifetime, the user-name with guest type will be deleted and the client associated with the guest user-name will be de-authenticated.
Step 7	**show running-config | section***user-name* **Example:** `Switch # show running-config | section guest`	Displays the configuration details.

Example

Configuring Mobility Agent (MA)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch # configure terminal`	Enters global configuration mode.
Step 2	**wireless mobility controller ip***mc-ipaddress* **public-ip** *mc-publicipaddress* **Example:** `Switch (config) # wireless mobility controller ip27.0.0.1 public-ip 27.0.0.1`	Configures the Mobility Controller to which the MA will be associated.
Step 3	**wlan** *wlan-name wlan-id ssid* **Example:** `Switch (config) # wlan mywlan 34 mywlan-ssid`	• For *wlan-name* enter, enter the profile name. The range is 1- 32 characters. • For *wlan-id*, enter the WLAN ID. The range is 1-512. • For *ssid*, enter the Service Set IDentifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID.
Step 4	**client vlan id***vlan-group name/vlan-id* **Example:** `Switch (config-wlan) # client vlan VLAN0136`	Configures the VLAN id or group of the WLAN.
Step 5	**no security wpa** **Example:** `Switch (config-wlan) # no security wpa`	The security configuration must be the same for the WLAN created on the GC. This example is for open authentication. For other security types such as open and webauth, appropriate command should be provided.
Step 6	**mobility anchor** *ipaddress* **Example:** `Switch (config-wlan) # mobility anchor 9.3.32.2`	Configures the Guest Controller as mobility anchor.
Step 7	**aaa-override** **Example:**	(Optional) Enables AAA override. AAA override is required for non open

	Command or Action	Purpose
	`Switch (config-wlan) # aaa-override`	authentication in case AAA attributes are to be prioritized. It is required only in case guest user need to be deauthenticated after lifetime or have to give aaa-override attribute to the user.
Step 8	**no shutdown** **Example:** `Switch(config-wlan) # no shutdown`	Enables the WLAN.
Step 9	**end** **Example:** `Switch (config) # end`	Returns to privileged EXEC mode.
Step 10	**show wireless mobility summary** **Example:** `Switch # show wireless mobility summary`	Verifies the mobility controller IP address and mobility tunnel status.
Step 11	**show wlan name** *wlan-name/id* **Example:** `Switch # show wlan name mywlan`	Displays the configuration of mobility anchor.

Example

Configuring Mobility Controller

Mobility Controller mode should be enabled using the **wireless mobility controller** command.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch # configure terminal`	Enters global configuration mode.
Step 2	**wireless mobility group member ip** *ip-address* **public-ip** *ip-address* **group** *group-name* **Example:** `Switch (config) # wireless mobility group member ip 27.0.0.1 public-ip 23.0.0.1 group test`	Adds all peers within the MC group. The *ip-address* should be the guest controller's IP address.
Step 3	**wireless mobility controller peer-group** *peer-group-name*	Creates the switch peer group.

	Command or Action	Purpose
	Example: `Switch (config) # wireless mobility controller peer-group pg`	
Step 4	**wireless mobility controller peer-group** *peer-group-name* **member ip** *ipaddress* **public-ip** *ipaddress* **Example:** `Switch (config) # wireless mobility controller peer-group pg member ip 9.7.136.10 public-ip 9.7.136.10`	Adds the MA to the switch peer group.
Step 5	**end** **Example:** `Switch (config) # end`	Returns to privileged EXEC mode.
Step 6	**show wireless mobility summary** **Example:** `Switch # show wireless mobility summary`	Displays the configuration details.

Example

Obtaining a Web Authentication Certificate

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch # configure terminal`	Enters global configuration mode.
Step 2	**crypto pki import** *trustpoint name* **pkcs12 tftp:** *passphrase* **Example:** `Switch (config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapserver-cert.p12 cisco`	Imports certificate.
Step 3	**end** **Example:** `Switch (config)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 4	**show crypto pki** *trustpoints cert* **Example:** `Switch # show crypto pki trustpoints cert`	Displays the configuration details.

Example

Displaying a Web Authentication Certificate

Procedure

	Command or Action	Purpose
Step 1	**show crypto ca certificate verb** **Example:** `Switch # show crypto ca certificate verb`	Displays the current web authentication certificate details.

Example

Choosing the Default Web Authentication Login Page

AAA override flag should be enabled on the WLAN for web authentication using local or remote AAA server.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch # configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth** *parameter-map name* **Example:** `Switch (config) # parameter-map type webauth test`	Configures the web-auth parameter-map.
Step 3	**wlan** *wlan-name* **Example:** `Switch (config) # wlan wlan10`	For the wlan-name, enter the profile name. The range is 1- 32 characters.
Step 4	**shutdown**	Disables WLAN.

	Command or Action	Purpose
	Example: `Switch (config) # shutdown`	
Step 5	**security web-auth** **Example:** `Controller (config-wlan) # security web-auth`	Enables web-auth on WLAN.
Step 6	**security web-auth authentication-list** *authentication list name* **Example:** `Controller (config-wlan) # security web-auth authentication-list test`	Allows you to map the authentication list name with the web-auth WLAN.
Step 7	**security web-auth parameter-map** *parameter-map name* **Example:** `Switch (config) # security web-auth parameter-map test`	Allows you to map the parameter-map name with the web-auth WLAN.
Step 8	**no shutdown** **Example:** `Switch (config) # no shutdown`	Enables the WLAN.
Step 9	**end** **Example:** `Switch (config) # end`	Returns to privileged EXEC mode.
Step 10	**show running-config | section** *wlan-name* **Example:** `Switch# show running-config | section mywlan`	Displays the configuration details.
Step 11	**show running-config | section parameter-map type webauth** *parameter-map* **Example:** `Switch# show running-config | section parameter-map type webauth test`	Displays the configuration details.

Example

Choosing a Customized Web Authentication Login Page from an External Web Server

AAA override flag should be enabled on the WLAN for web authentication using local or remote AAA server.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch # configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth global** **Example:** `Switch (config) # parameter-map type webauth global`	Configures a global webauth type parameter.
Step 3	**virtual-ip {ipv4 | ipv6}** *ip-address* **Example:** `Switch (config-params-parameter-map) # virtual-ip ipv4 1.1.1.1`	Configures the virtual IP address.
Step 4	**parameter-map type webauth** *parameter-map name* **Example:** `Switch (config-params-parameter-map) # parameter-map type webauth test`	Configures the webauth type parameter.
Step 5	**type {authbypass | consent | webauth | webconsent}** **Example:** `Switch (config-params-parameter-map) # type webauth`	Configures webauth subtypes such as consent, passthru, webauth, or webconsent.
Step 6	**redirect [for-login|on-success|on-failure]** *URL* **Example:** `Switch (config-params-parameter-map) # redirect for-login http://9.1.0.100/login.html`	Configures the redirect URL for the log in page, success page, and failure page.
Step 7	**redirect portal {ipv4 | ipv6}** *ip-address* **Example:** `Switch (config-params-parameter-map) # redirect portal ipv4`	Configures the external portal IPv4 address.

	Command or Action	Purpose
Step 8	**end** **Example:** `Switch (config-params-parameter-map) # end`	Returns to privileged EXEC mode.
Step 9	show running-config | section parameter-map **Example:** `Switch # show running-config | section parameter-map`	Displays the configuration details.

Example

Assigning Login, Login Failure, and Logout Pages per WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch # configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth** *parameter-map-name* **Example:** `Switch (config) # parameter-map type webauth test`	Configures the webauth type parameter.
Step 3	**custom-page login device** *html-filename* **Example:** `Switch (config-params-parameter-map)# custom-page login device device flash:login.html`	Allows you to specify the filename for web authentication customized login page.
Step 4	**custom-page login expired** *html-filename* **Example:** `Switch (config-params-parameter-map)# custom-page login expired device flash:loginexpired.html`	Allows you to specify the filename for web authentication customized login expiry page.
Step 5	**custom-page failure device** *html-filename* **Example:** `Switch (config-params-parameter-map)# custom-page failure device device flash:loginfail.html`	Allows you to specify the filename for web authentication customized login failure page.

	Command or Action	Purpose
Step 6	**custom-page success device** *html-filename* **Example:** `Switch (config-params-parameter-map)# custom-page success device device flash:loginsuccess.html`	Allows you to specify the filename for web authentication customized login success page.
Step 7	**end** **Example:** `Switch (config-params-parameter-map)# end`	Returns to privileged EXEC mode.
Step 8	**show running-config | section parameter-map type webauth** *parameter-map* **Example:** `Switch (config) # show running-config | section parameter-map type webauth test`	Displays the configuration details.

Example

Configuring AAA-Override

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch # configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name* **Example:** `Switch (config) # wlan ramban`	For *wlan-name*, enter the profile name. The range is 1- 32 characters.
Step 3	**aaa-override** **Example:** `Switch (config-wlan) # aaa-override`	Enables AAA override on the WLAN.
Step 4	**end** **Example:** `Switch (config-wlan) # end`	Returns to privileged EXEC mode.
Step 5	**show running-config | section** *wlan-name* **Example:**	Displays the configuration details.

	Command or Action	Purpose
	`Switch # show running-config | section ramban`	

Example

Configuring Client Load Balancing

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch # configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name* **Example:** `Switch (config)# wlan ramban`	For *wlan-name*, enter the profile name.
Step 3	**shutdown** **Example:** `Switch (config-wlan)# shutdown`	Disables WLAN.
Step 4	**mobility anchor** *ip-address1* **Example:** `Switch (config-wlan) # mobility anchor 9.7.136.15`	Configures a guest controller as mobility anchor.
Step 5	**mobility anchor** *ip-address2* **Example:** `Switch (config-wlan) # mobility anchor 9.7.136.16`	Configures a guest controller as mobility anchor.
Step 6	**no shutdown wlan** **Example:** `Switch (config-wlan) # no shutdown wlan`	Enables the WLAN.
Step 7	**end** **Example:** `Switch (config-wlan) # end`	Returns to privileged EXEC mode.
Step 8	**show running-config | section** *wlan-name* **Example:**	Displays the configuration details.

	Command or Action	Purpose
	`Switch # show running-config | section ramban`	

Example

Configuring Preauthentication ACL

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name* **Example:** `Switch (config)# wlan ramban`	For *wlan-name*, enter the profile name.
Step 3	**shutdown** **Example:** `Switch (config-wlan)# shutdown`	Disables the WLAN.
Step 4	**ip access-group web** *preauthrule* **Example:** `Switch (config-wlan)# ip access-group web preauthrule`	Configures ACL that has to be applied before authentication.
Step 5	**no shutdown** **Example:** `Switch (config)# no shutdown`	Enables the WLAN.
Step 6	**end** **Example:** `Switch (config-wlan)# end`	Returns to privileged EXEC mode.
Step 7	**show wlan name** *wlan-name* **Example:** `Switch# show wlan name ramban`	Displays the configuration details.

Example

Configuring IOS ACL Definition

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch # configure terminal`	Enters global configuration mode.
Step 2	**ip access-list extended** *access-list number* **Example:** `Switch (config) # ip access-list extended 102`	Configures extended IP access-list.
Step 3	**permit udp any eq** *port number* **any** **Example:** `Switch (config-ext-nacl) # permit udp any eq 8080 any`	Configures destination host.
Step 4	**end** **Example:** `Switch (config-wlan) # end`	Returns to privileged EXEC mode.
Step 5	**show access-lists** *ACL number* **Example:** `Switch # show access-lists 102`	Displays the configuration details.

Example

Configuring Webpassthrough

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch # configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**parameter-map type webauth** *parameter-map name* **Example:** `Switch (config) # parameter-map type webauth webparalocal`	Configures the webauth type parameter.
Step 3	**type consent** **Example:** `Switch (config-params-parameter-map) # type consent`	Configures webauth type as consent.
Step 4	**end** **Example:** `Switch (config-params-parameter-map) # end`	Returns to privileged EXEC mode.
Step 5	**show running-config | section parameter-map type webauth** *parameter-map* **Example:** `Switch (config) # show running-config | section parameter-map type webauth test`	Displays the configuration details.

Example

Configuration Examples for Guest Access

Example: Creating a Lobby Ambassador Account

This example shows how to configure a lobby ambassador account.

```
Switch# configure terminal
Switch(config)# user-name lobby
Switch(config)# type lobby-admin
Switch(config)# password 0 lobby
Switch(config)# end
Switch#  show running-config | section lobby
    user-name lobby
    creation-time 1351118727
    password 0 lobby
    type lobby-admin
```

Example: Obtaining Web Authentication Certificate

This example shows how to obtain web authentication certificate.

```
Switch# configure terminal
Switch(config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapserver-cert.p12 cisco
Switch(config)# end
Switch# show crypto pki trustpoints cert
 Trustpoint cert:
    Subject Name:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
          Serial Number (hex): 00
    Certificate configured.
Switch# show  crypto pki certificates cert
Certificate
  Status: Available
  Certificate Serial Number (hex): 04
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Subject:
    Name: ldapserver
    e=rkannajr@cisco.com
    cn=ldapserver
    ou=WNBU
    o=Cisco
    st=California
    c=US
  Validity Date:
    start date: 07:35:23 UTC Jan 31 2012
    end   date: 07:35:23 UTC Jan 28 2022
  Associated Trustpoints: cert ldap12
  Storage: nvram:rkannajrcisc#4.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 00
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Subject:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Validity Date:
```

```
    start date: 07:27:56 UTC Jan 31 2012
    end   date: 07:27:56 UTC Jan 28 2022
  Associated Trustpoints: cert ldap12 ldap
  Storage: nvram:rkannajrcisc#0CA.cer
```

Example: Displaying a Web Authentication Certificate

This example shows how to display a web authentication certificate.

```
Switch# show crypto ca certificate verb
     Certificate
     Status: Available
     Version: 3
     Certificate Serial Number (hex): 2A9636AC00000000858B
     Certificate Usage: General Purpose
     Issuer:
    cn=Cisco Manufacturing CA
    o=Cisco Systems
    Subject:
    Name: WS-C3780-6DS-S-2037064C0E80
    Serial Number: PID:WS-C3780-6DS-S SN:FOC1534X12Q
    cn=WS-C3780-6DS-S-2037064C0E80
    serialNumber=PID:WS-C3780-6DS-S SN:FOC1534X12Q
    CRL Distribution Points:
    http://www.cisco.com/security/pki/crl/cmca.crl
    Validity Date:
    start date: 15:43:22 UTC Aug 21 2011
    end   date: 15:53:22 UTC Aug 21 2021
    Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
    Signature Algorithm: SHA1 with RSA Encryption
    Fingerprint MD5: A310B856 A41565F1 1D9410B5 7284CB21
    Fingerprint SHA1: 04F180F6 CA1A67AF 9D7F561A 2BB397A1 0F5EB3C9
    X509v3 extensions:
    X509v3 Key Usage: F0000000
      Digital Signature
      Non Repudiation
      Key Encipherment
      Data Encipherment
    X509v3 Subject Key ID: B9EEB123 5A3764B4 5E9C54A7 46E6EECA 02D283F7
    X509v3 Authority Key ID: D0C52226 AB4F4660 ECAE0591 C7DC5AD1 B047F76C
    Authority Info Access:
    Associated Trustpoints: CISCO_IDEVID_SUDI
    Key Label: CISCO_IDEVID_SUDI
```

Example: Configuring Guest User Accounts

This example shows how to configure a guest user account.

```
Switch# configure terminal
Switch(config)# user-name guest
Switch(config-user-name)# password 0 guest
Switch(config-user-name)# type network-user description guest guest-user lifetime year 1
month 10 day 3 hour 1 minute 5 second 30
Switch(config-user-name)# end
Switch# show aaa local netuser all
```

```
User-Name           : guest
Type                : guest
Password            : guest
Is_passwd_encrypted : No
Descriptio          : guest
Attribute-List      : Not-Configured
First-Login-Time    : Not-Logged-In
Num-Login           : 0
Lifetime            : 1 years 10 months 3 days 1 hours 5 mins 30 secs
Start-Time          : 20:47:37 chennai Dec 21 2012
```

Example: Configuring Mobility Controller

This example shows how to configure a mobility controller.

```
Switch# configure terminal
Switch(config)# wireless mobility group member ip 27.0.0.1 public-ip 23.0.0.1 group test
Switch(config)# wireless mobility controller peer-group pg
Switch(config)# wireless mobility controller peer-group pg member ip 9.7.136.10 public-ip
9.7.136.10
Switch(config)# end
Switch# show wireless mobility summary

Mobility Controller Summary:

Mobility Role                                 : Mobility Controller
Mobility Protocol Port                        : 16666
Mobility Group Name                           : default
Mobility Oracle                               : Enabled
DTLS Mode                                     : Enabled

Mobility Keepalive Interval                   : 10
Mobility Keepalive Count                      : 3
Mobility Control Message DSCP Value           : 7
Mobility Domain Member Count                  : 3

Link Status is Control Link Status : Data Link Status

Controllers configured in the Mobility Domain:

IP              Public IP        Group Name       Multicast IP     Link Status
------------------------------------------------------------------------------
9.9.9.2         -                default          0.0.0.0          UP   : UP
12.12.11.11     12.13.12.12      rasagna-grp                       DOWN : DOWN
27.0.0.1        23.0.0.1         test                              DOWN : DOWN

Switch Peer Group Name            : spg1
Switch Peer Group Member Count    : 0
Bridge Domain ID                  : 0
Multicast IP Address              : 0.0.0.0

Switch Peer Group Name            : pg
Switch Peer Group Member Count    : 1
Bridge Domain ID                  : 0
Multicast IP Address              : 0.0.0.0

IP              Public IP            Link Status
------------------------------------------------
9.7.136.10      9.7.136.10           DOWN : DOWN
```

Example: Choosing the Default Web Authentication Login Page

This example shows how to choose a default web authentication login page.

```
Switch# configure terminal
Switch(config)# parameter-map type webauth test
This operation will permanently convert all relevant authentication commands to their CPL
control-policy equivalents. As this conversion is irreversible and will
disable the conversion CLI 'authentication display [legacy|new-style]', you are strongly
advised to back up your current configuration before proceeding.
Do you wish to continue? [yes]: yes
Switch(config)# wlan wlan50
Switch(config-wlan)# shutdown
Switch(config-wlan)# security web-auth authentication-list test
Switch(config-wlan)# security web-auth parameter-map test
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
Switch# show running-config | section wlan50
wlan wlan50 50 wlan50
 security wpa akm cckm
 security wpa wpa1
 security wpa wpa1 ciphers aes
 security wpa wpa1 ciphers tkip
 security web-auth authentication-list test
 security web-auth parameter-map test
 session-timeout 1800
 no shutdown

Switch# show running-config | section parameter-map type webauth test
parameter-map type webauth test
 type webauth
```

Example: Choosing a Customized Web Authentication Login Page from an IPv4 External Web Server

This example shows how to choose a customized web authentication login page from an IPv4 external web server.

```
Switch# configure terminal
Switch(config)# parameter-map type webauth global
Switch(config-params-parameter-map)# virtual-ip ipv4 1.1.1.1
Switch(config-params-parameter-map)# parameter-map type webauth test
Switch(config-params-parameter-map)# type webauth
Switch(config-params-parameter-map)# redirect for-login http://9.1.0.100/login.html
Switch(config-params-parameter-map)# redirect portal ipv4 9.1.0.100
Switch(config-params-parameter-map)# end
Switch# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv4 1.1.1.1
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 9.1.0.100
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test
```

Example: Assigning Login, Login Failure, and Logout Pages per WLAN

This example shows how to assign login, login failure and logout pages per WLAN.

```
Switch# configure terminal
Switch(config)# parameter-map type webauth test
Switch(config-params-parameter-map)# custom-page login device flash:loginsantosh.html
Switch(config-params-parameter-map)# custom-page login expired device flash:loginexpire.html
Switch(config-params-parameter-map)# custom-page failure device flash:loginfail.html
Switch(config-params-parameter-map)# custom-page success device flash:loginsucess.html
Switch(config-params-parameter-map)# end
Switch# show running-config | section parameter-map type webauth test
 parameter-map type webauth test
 type webauth
 redirect for-login http://9.1.0.100/login.html
 redirect portal ipv4 9.1.0.100
 custom-page login device flash:loginsantosh.html
 custom-page success device flash:loginsucess.html
 custom-page failure device flash:loginfail.html
 custom-page login expired device flash:loginexpire.html
```

Example: Configuring AAA-Override

This example shows how to configure aaa-override.

```
Switch# configure terminal
Switch(config)# wlan fff
Switch(config-wlan)# aaa-override
Switch(config-wlan)# end
Switch# show running-config | section fff
 wlan fff 44 fff
 aaa-override
 shutdown
```

Example: Configuring Client Load Balancing

This example shows how to configure client load balancing.

```
Switch# configure terminal
Switch(config)# wlan fff
Switch(config-wlan)# shutdown
Switch(config-wlan)# mobility anchor 9.7.136.15
Switch(config-wlan)# mobility anchor 9.7.136.16
Switch(config-wlan)# no shutdown wlan
Switch(config-wlan)# end
Switch# show running-config | section fff
wlan fff 44 fff
 aaa-override
 shutdown
```

Example: Configuring Preauthentication ACL

This example shows how to configure preauthentication ACL.

```
Switch# configure terminal
Switch(config)# wlan fff
Switch(config-wlan)# shutdown
Switch(config-wlan)# ip access-group web preauthrule
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
Switch# show wlan name fff
```

Example: Configuring IOS ACL Definition

This example shows how to configure IOS ACL definition.

```
Switch# configure terminal
Switch(config)# ip access-list extended 102
Switch(config-ext-nacl)# permit udp any eq 8080 any
Switch(config-ext-nacl)# end
Switch# show access-lists 102
 Extended IP access list 102
    10 permit udp any eq 8080 any
```

Example: Configuring Webpassthrough

This example shows how to configure webpassthrough.

```
Switch# configure terminal
Switch(config)# parameter-map type webauth webparalocal
Switch(config-params-parameter-map)# type consent
Switch(config-params-parameter-map)# end
Switch# show running-config | section parameter-map type webauth test
 parameter-map type webauth test
 type webauth
 redirect for-login http://9.1.0.100/login.html
 redirect portal ipv4 9.1.0.100
```

Additional References for Guest Access

Related Documents

Related Topic	Document Title
Mobility CLI commands	*Mobility Command Reference, Cisco IOS XE 3SE (Cisco WLC 5700 Series)*
Mobility configuration	*Mobility Configuration Guide, Cisco IOS XE 3SE (Cisco WLC 5700 Series)*
Security CLI commands	*Security Command Reference, Cisco IOS Release 3SE (Cisco WLC 5700 Series)*
Configuring web-based authentication on the Catalyst 5700 Series Wireless Controller	*Security Configuration Guide, Cisco IOS Release 3SE (Cisco WLC 5700 Series)*

Related Topic	Document Title
Wired guest access configuration and commands	*Identity Based Networking Services*

Standards and RFCs

Standard/RFC	Title
None	-

MIBs

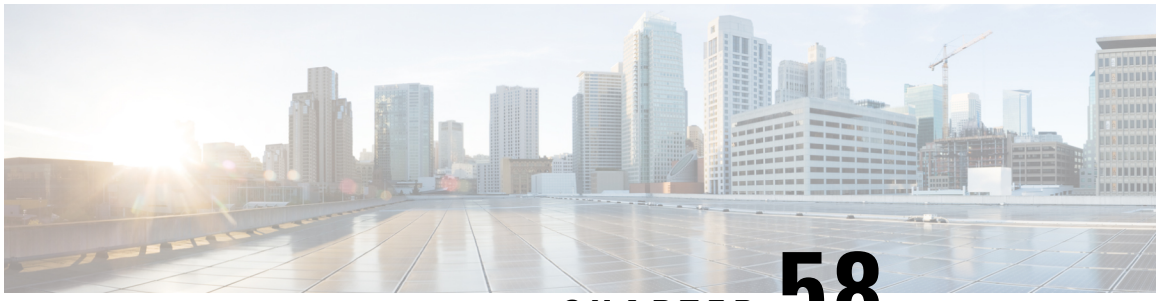
MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for Guest Access

Releases	Feature Information
Cisco IOS XE Release 3.2SE	This feature was introduced.



CHAPTER 58

Managing Rogue Devices

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Rogue Devices

Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain-text or other denial-of-service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as usernames and passwords. The hacker can then transmit a series of Clear to Send (CTS) frames. This action mimics an access point, informing a particular client to transmit, and instructing all the other clients to wait, which results in legitimate clients being unable to access network resources. Wireless LAN service providers have a strong interest in banning rogue access points from the air space.

Because rogue access points are inexpensive and readily available, employees sometimes plug unauthorized rogue access points into existing LANs and build ad hoc wireless networks without their IT department's knowledge or consent. These rogue access points can be a serious breach of network security because they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to

intercept network traffic and hijack client sessions. There is an increased chance of enterprise security breach when wireless users connect to access points in the enterprise network.

The following are some guidelines to manage rogue devices:

- The containment frames are sent immediately after the authorization and associations are detected. The enhanced containment algorithm provides more effective containment of ad hoc clients.
- In a dense RF environment, where maximum rogue access points are suspected, the chances of detecting rogue access points by a local mode access point in channel 157 or channel 161 is less when compared to other channels. To mitigate this problem, we recommend that you use dedicated monitor mode access points.
- The local mode access points are designed to serve associated clients. These access points spend relatively less time performing off-channel scanning: about 50 milliseconds on each channel. If you want to perform high rogue detection, a monitor mode access point must be used. Alternatively, you can reduce the scan intervals from 180 seconds to a lesser value, for example, 120 or 60 seconds, ensuring that the radio goes off-channel more frequently, which improves the chances of rogue detection. However, the access point will still spend about 50 milliseconds on each channel.
- Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices.
- Client card implementations might mitigate the effectiveness of ad hoc containment.
- It is possible to classify and report rogue access points through the use of rogue states and user-defined classification rules that enable rogues to automatically move between states.
- Each controller limits the number of rogue containment to three per radio (or six per radio for access points in the monitor mode).
- Rogue Location Discovery Protocol (RLDP) detects rogue access points that are configured for open authentication.
- RLDP detects rogue access points that use a broadcast Basic Service Set Identifier (BSSID), that is, the access point broadcasts its Service Set Identifier in beacons.
- RLDP detects only those rogue access points that are on the same network. If an access list in the network prevents the sending of RLDP traffic from the rogue access point to the controller, RLDP does not work.
- RLDP does not work on 5-GHz Dynamic Frequency Selection (DFS) channels. However, RLDP works when the managed access point is in the monitor mode on a DFS channel.
- If RLDP is enabled on mesh APs, and the APs perform RLDP tasks, the mesh APs are dissociated from the controller. The workaround is to disable RLDP on mesh APs.
- If RLDP is enabled on non-monitor APs, client connectivity outages occur when RLDP is in process.
- If the rogue is manually contained, the rogue entry is retained even after the rogue expires.
- If the rogue is contained by any other means, such as auto, rule, and AwIPS preventions, the rogue entry is deleted when it expires.
- The controller will request to AAA server for rogue client validation only once. As a result, if rogue client validation fails on the first attempt then the rogue client will not be detected as a threat any more. To avoid this, add the valid client entries in the authentication server before enabling **Validate Rogue Clients Against AAA**.

- All the valid client MAC details should be registered in the AAA authentication server with the same MAC delimiter options as set in the RADIUS configuration on the controller. For more information about configuring MAC delimiter options, see the Configuring RADIUS (GUI) section.
- In the 7.4 and earlier releases, if a rogue that was already classified by a rule was not reclassified. In the 7.5 release, this behavior is enhanced to allow reclassification of rogues based on the priority of the rogue rule. The priority is determined by using the rogue report that is received by the controller.
- All rogues that are marked as friendly or contained state (due to auto or rule or manual) are stored in the flash memory of the controller. When you reboot the controller loaded with Release 7.4, these rogues are shown as manually changed. If you wish to reboot the controller, you need to clear all rogue APs and rogue adhoc from the controller, save the configuration, and then reboot the controller.
- All rogues that are marked as friendly or contained state (only due to manual) are stored in the flash memory of the controller. If you upgrade the controller from the Release 7.4 to 7.6 or later versions, then all rogues stored in the Release 7.4 are shown as manually classified (if friendly classified) or manually contained. Hence after upgrading the controller from the Release 7.4 to 7.6 or later versions, you need to delete all rogue APs and rogue adhoc from the controller and then start configuring rogue detection.
- A FlexConnect AP (with rogue detection enabled) in the connected mode takes the containment list from the controller. If auto-contain SSID and auto contain adhoc are set in the controller, then these configurations are set to all FlexConnect APs in the connected mode and the AP stores it in its memory.

  When the FlexConnect AP moves to a standalone mode, the following tasks are performed:

  - The containment set by the controller continues.
  - If the FlexConnect AP detects any rogue AP that has same SSID as that of infra SSID (SSID configured in the controller that the FlexConnect AP is connected to), then containment gets started if auto contain SSID was enabled from the controller before moving to the standalone mode.
  - If the FlexConnect AP detects any adhoc rogue, containment gets started if **auto-contain adhoc** was enabled from the controller when it was in the connected mode.

  When the standalone FlexConnect AP moves back to the connected mode, then the following tasks are performed:

  - All containment gets cleared.
  - Containment initiated from the controller will take over.

- The rogue detector AP fails to co-relate and contain the wired rogue AP on a 5Mhz channel because the MAC address of the rogue AP for WLAN, LAN, 11a radio and 11bg radio are configured with a difference of +/-1 of the rogue BSSID. In the 8.0 release, this behavior is enhanced by increasing the range of MAC address, that the rogue detector AP co-relates the wired ARP MAC and rogue BSSID, by +/-3.
- The rogue access points with open authentication can be detected on wire. The NAT wired or rogue wired detection is not supported in by WLC (both RLDP and rogue detector AP). The non-adjacent MAC address is supported by rogue detector mode of AP and not by RLDP.
- In a High Availability scenario, if the rogue detection security level is set to either High or Critical, the rogue timer on the standby Cisco WLC starts only after the rogue detection pending stabilization time, which is 300 seconds. Therefore, the active configurations on the standby Cisco WLC are reflected only after 300 seconds.

- After an AP is moved from rogue detection mode to any other mode, the rogue detection functionality is not retained on the AP. To enable rogue detection functionality on the AP, you have to explicitly move the AP to the rogue detection mode.

Note A rogue AP or client or adhoc containment configuration is not saved after the reload. You have to configure all the rogues again after the reload.

Note No separate command exists for controlling rogue client traps. However, you can enable or disable rogue client traps using the **config trapflags rogueap** {**enable** | **disable**} command, which is also used for rouge APs. In GUI configuration also, you should use the rogue AP flag under **Management** > **SNMP** > **TrapControl** > **Security** > **Rogue AP** to control rogue clients.

Rogue Location Discovery Protocol

Rogue Location Discovery Protocol (RLDP) is an active approach, which is used when rogue AP has no authentication (Open Authentication) configured. This mode, which is disabled by default, instructs an active AP to move to the rogue channel and connect to the rogue as a client. During this time, the active AP sends de-authentication messages to all connected clients and then shuts down the radio interface. Then, it associates to the rogue AP as a client. The AP then tries to obtain an IP address from the rogue AP and forwards a User Datagram Protocol (UDP) packet (port 6352) that contains the local AP and rogue connection information to the controller through the rogue AP. If the controller receives this packet, the alarm is set to notify the network administrator that a rogue AP was discovered on the wired network with the RLDP feature.

RLDP has 100 % accuracy in rouge AP detection. It detects Open APs and NAT APs.

Note Use the **debug dot11 rldp enable** command in order to check if the Lightweight AP associates and receives a DHCP address from the rogue AP. This command also displays the UDP packet sent by the Lightweight AP to the controller.

A sample of a UDP (destination port 6352) packet sent by the Lightweight AP is shown here: 0020 0a 01 01 0d 0a 01 .....(.*..... 0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00 .....x..... 0040 00 00 00 00 00 00 00 00 00 00 00 00

The first 5 bytes of the data contain the DHCP address given to the local mode AP by the rogue AP. The next 5 bytes are the IP address of the controller, followed by 6 bytes that represent the rogue AP MAC address. Then, there are 18 bytes of zeroes.

The following steps describe the functioning of RLDP:

1. Identify the closest Unified AP to the rogue using signal strength values.
2. The AP then connects to the rogue as a WLAN client, attempting three associations before timing out.
3. If association is successful, the AP then uses DHCP to obtain an IP address.
4. If an IP address was obtained, the AP (acting as a WLAN client) sends a UDP packet to each of the controller's IP addresses.

5. If the controller receives even one of the RLDP packets from the client, that rogue is marked as on-wire.

Note The RLDP packets are unable to reach the controller if filtering rules are placed between the controller's network and the network where the rogue device is located.

Caveats of RLDP:

- RLDP only works with open rogue APs broadcasting their SSID with authentication and encryption disabled.
- RLDP requires that the Managed AP acting as a client is able to obtain an IP address via DHCP on the rogue network.
- Manual RLDP can be used to attempt an RLDP trace on a rogue multiple number of times.
- During RLDP process, the AP is unable to serve clients. This negatively impacts performance and connectivity for local mode APs. To avoid this case, RLDP can be selectively enabled for Monitor Mode AP only.
- RLDP does not attempt to connect to a rogue AP operating in a 5GHz DFS channel.

Note RLDP is not supported for use with Cisco autonomous rogue access points. These access points drop the DHCP Discover request sent by the RLDP client. Also, RLDP is not supported if the rogue access point channel requires dynamic frequency selection (DFS). If the automatic RLDP attempt does not detect the rogue (due to a noisy RF environment, for example), the controller does not retry. However, you can initiate RLDP manually on a rogue device.

Detecting Rogue Devices

The controller continuously monitors all the nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) and the rogue detector mode access point is connected to determine if the rogue is attached to your network.

Controller initiates RLDP on rogue devices that have open authenticated and configured. If RLDP uses Flexconnect or local mode access points, then clients are disconnected for that moment. After the RLDP cycle, the clients are reconnected to the access points. As and when rogue access points are seen (auto-configuration), the RLDP process is initiated.

You can configure the controller to use RLDP on all the access points or only on the access points configured for the monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded radio frequency (RF) space, allowing monitoring without creating unnecessary interference and without affecting the regular data access point functionality. If you configure the controller to use RLDP on all the access points, the controller always chooses the monitor access point for RLDP operation if a monitor access point and a local (data) access point are both nearby. If RLDP determines that the rogue is on your network, you can choose to contain the detected rogue either manually or automatically.

RLDP detects on wire presence of the rogue access points that are configured with open authentication only once, which is the default retry configuration. Retries can be configured using the **config rogue ap rldp retries** command.

You can initiate or trigger RLDP from controller in three ways:

1. Enter the RLDP initiation command manually from the controller CLI. The equivalent GUI option for initiating RLDP is not supported.

   config rogue ap rldp initiate *mac-address*

2. Schedule RLDP from the controller CLI. The equivalent GUI option for scheduling RLDP is not supported.

   config rogue ap rldp schedule

3. Auto RLDP. You can configure auto RLDP on controller either from controller CLI or GUI but keep in mind the following guidelines:

   - The auto RLDP option can be configured only when the rogue detection security level is set to custom.
   - Either auto RLDP or schedule of RLDP can be enabled at a time.

A rogue access point is moved to a contained state either automatically or manually. The controller selects the best available access point for containment and pushes the information to the access point. The access point stores the list of containments per radio. For auto containment, you can configure the controller to use only the monitor mode access point. The containment operation occurs in the following two ways:

- The container access point goes through the list of containments periodically and sends unicast containment frames. For rogue access point containment, the frames are sent only if a rogue client is associated.
- Whenever a contained rogue activity is detected, containment frames are transmitted.

Individual rogue containment involves sending a sequence of unicast disassociation and deauthentication frames.

Cisco Prime Infrastructure Interaction and Rogue Detection

Cisco Prime Infrastructure supports rule-based classification and uses the classification rules configured on the controller. The controller sends traps to Cisco Prime Infrastructure after the following events:

- If an unknown access point moves to the Friendly state for the first time, the controller sends a trap to Cisco Prime Infrastructure only if the rogue state is Alert. It does not send a trap if the rogue state is Internal or External.
- If a rogue entry is removed after the timeout expires, the controller sends a trap to Cisco Prime Infrastructure for rogue access points categorized as Malicious (Alert, Threat) or Unclassified (Alert). The controller does not remove rogue entries with the following rogue states: Contained, Contained Pending, Internal, and External.

Validating Rogue Devices Using MSE

You can validate the rogue clients by utilizing the resources available in the Cisco Mobility Services Engine (MSE). Using MSE, you can dynamically list the clients joining to the switch. The list of clients joined to the switch is stored in the MSE as a centralized location, where the switch communicates with MSE and validates the client before reporting if the rogue client is a valid one or not. MSE maintains the MAC addresses of clients joined to the switch for a period of 7 days and this time period is non-configurable. After enabling rouge validation on the switch, the NMSP communication is triggered. Only after this, the switch communicates with MSE. When MSE stops responding for 60 seconds or more, the MSE validation stops, and resumes with NSMP communication.

The communication between the switch and MSE is an on-demand service as the switch requests this service from MSE.

- NMSP request messages and response messages are exchanged between the switch and MSE as an on-demand service.
- The switch passes the MAC addresses of the detected rogue clients to MSE using the NMSP request message.
- MSE validates the rogue client and passes the response back to the switch using NMSP response message.
- Upon validating the response against the configuration settings, the switch performs either one of the following actions on the rogue client: contain, alarm, or ignore.

How to Configure Rogue Detection

Configuring Rogue Detection (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps rogue detection min-rssi** *rssi in dBm* **Example:** `Switch(config)# wireless wps rogue detection min-rssi 100`	Specify the minimum RSSI value that rogues should have for APs to detect and for rogue entry to be created in the switch. Valid range for the rssi in dBm parameter is –128 dBm to -70 dBm, and the default value is -128 dBm. **Note** This feature is applicable to all the AP modes. There can be many rogues with very weak RSSI values that do not provide any valuable information in rogue analysis. Therefore, you can use this option to filter rogues by specifying the minimum RSSI value at which APs should detect rogues.
Step 3	**wireless wps rogue detection min-transient-time** *time in seconds* **Example:**	Specify the time interval at which rogues have to be consistently scanned for by APs after the first time the rogues are scanned.

	Command or Action	Purpose
	`Switch(config)# wireless wps rogue detection min-transient-time`	Valid range for the time in sec parameter is 120 seconds to 1800 seconds, and the default value is 0. **Note** This feature is applicable to APs that are in monitor mode only. Using the transient interval values, you can control the time interval at which APs should scan for rogues. APs can also filter the rogues based on their transient interval values. This feature has the following advantages: • Rogue reports from APs to the controller are shorter • Transient rogue entries are avoided in the controller • Unnecessary memory allocation for transient rogues are avoided

Step 4	**wireless wps rogue client** {**aaa** | **mse**}
	Example:
	`Switch(config)# wireless wps rogue client aaa`
	`Switch(config)# wireless wps rogue client mse`
		Set the AAA server or local database, or the MSE to validate if rogue clients are valid clients.

Step 5	**wireless wps rogue ap valid-client auto-contain** **Example:** `Switch(config)# wireless wps rogue ap valid-client auto-contain`	Specify to automatically contain a rogue access point to which trusted clients are associated.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Rogue Detection (GUI)

Procedure

Step 1 Make sure that rogue detection is enabled on the corresponding access points. Rogue detection is enabled by default for all access points joined to the controller (except for OfficeExtend access points). However, you can enable or disable rogue detection for individual access point by choosing **Configuration** > **Wireless** > **Access Policies** > **All APs** to open Edit AP page, selecting or unselecting the **Rogue Detector** check box in the General area of the Edit AP page.

Step 2 Choose **Configuration** > **Security** > **Wireless Protection Policies** > **Rogue Policies**.

The **Rogue Policies** page is displayed.

Step 3 Choose one of the following options from the **Rogue Location Discovery Protocol** drop-down list:

- **Disable**—Disables RLDP on all the access points. This is the default value.
- **All APs**—Enables RLDP on all the access points.
- **Monitor Mode APs**—Enables RLDP only on the access points in the monitor mode.

Step 4 In the **Expiration Timeout for Rogue AP and Rogue Client Entries** text box, enter the number of seconds after which the rogue access point and client entries expire and are removed from the list. The valid range is 240 to 3600 seconds, and the default value is 1200 seconds.

Note If a rogue access point or client entry times out, it is removed from the controller only if its rogue state is Alert or Threat for any classification type.

Step 5 To use the AAA server or local database to validate if rogue clients are valid clients, select the **Validate Rogue Clients Against AAA** check box. By default, the check box is unselected.

Step 6 If necessary, select the **Detect and Report Adhoc Networks** check box to enable adhoc rogue detection and reporting. By default, the check box is selected.

Step 7 In the **Rogue Detection Report Interval** text box, enter the time interval, in seconds, at which APs should send the rogue detection report to the controller. The valid range is 10 seconds to 300 seconds, and the default value is 10 seconds.

Step 8 If you want the controller to automatically contain certain rogue devices, enable the following parameters. By default, these parameters are in disabled state.

Caution When you select any of the Auto Contain parameters and click **Apply**, the following message is displayed: "`Using this feature may have legal consequences. Do you want to continue?`" The 2.4-GHz and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

- **Auto Containment Level**—Set the auto containment level. By default, the auto containment level is set to **1**.
- **Auto Containment only for Monitor mode APs**—Configure the monitor mode access points for auto-containment.
- **Rogue on Wire**—Configure the auto containment of rogues that are detected on the wired network.

- **Using Our SSID**—Configure the auto containment of rogues that are advertising your network's SSID. If you leave this parameter unselected, the controller only generates an alarm when such a rogue is detected.
- **Valid Client on Rogue AP**—Configure the auto containment of a rogue access point to which trusted clients are associated. If you leave this parameter unselected, the controller only generates an alarm when such a rogue is detected.
- **Adhoc Rogue AP**—Configure the auto containment of adhoc networks detected by the controller. If you leave this parameter unselected, the controller only generates an alarm when such a network is detected.

Step 9 Click **Apply**.

Step 10 Click **Save Configuration**.

Monitoring Rogue Detection

This section describes the new command for rogue detection.

The following command can be used to monitor rogue detection on the switch.

Table 81: Monitoring Rogue Detection Command

Command	Purpose
show wireless wps rogue ap summary	Displays a list of all rogue access points detected by the switch.
show wireless wps rogue client detailed *client-mac*	Displays detailed information for a specific rogue client.
show wireless wps rogue client summary	Displays a list of all rogue clients detected by the switch.
show nmsp capability	Displays the NMSP capabilities.

Table 82: Monitoring Rogue Auto-Containment Information

Command	Purpose
show wireless wps rogue auto-contain	Displays the rogue auto-containment information.

Examples: Rogue Detection Configuration

This example shows how to configure the minimum RSSI that a detected rogue AP needs to be at, to have an entry created at the switch:

```
Switch# configure terminal
Switch(config)# wireless wps rogue detection min-rssi -100
```

```
Switch(config)# end
Switch# show wireless wps rogue client detailed/show wireless wps rogue ap summary
```

This example shows how to configure the classification interval:

```
Switch# configure terminal
Switch(config)# wireless wps rogue detection min-transient-time 500

Switch(config)# end
Switch# show wireless wps rogue client detailed/show wireless wps rogue ap summary
```

This example shows how to configure the MSE to validate if rogue clients are valid clients:

```
Switch# configure terminal
Switch(config)# wireless wps rogue client mse
Switch(config)# end
Switch# show wireless wps rogue client summary
```

This example shows how to automatically contain a rogue access point to which trusted clients are associated:

```
Switch# configure terminal
Switch(config)# wireless wps rogue ap valid-client auto-contain
Switch(config)# end
Switch# show wireless wps rogue ap summary
Switch# show nmsp capability
```

Additional References for Rogue Detection

Related Documents

Related Topic	Document Title
Security commands	*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

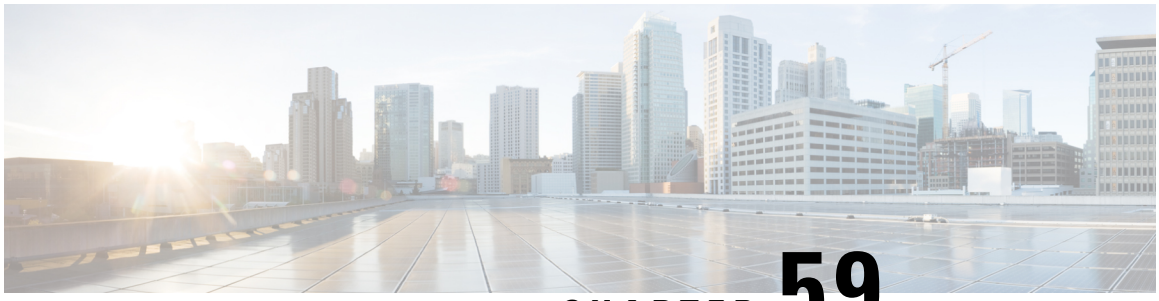
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Performing Rogue Detection Configuration

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.
Cisco IOS XE 3E	Rogue validation against MSE.



CHAPTER 59

Classifying Rogue Access Points

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Classifying Rogue Access Points

The controller software enables you to create rules that can organize and display rogue access points as Friendly, Malicious, or Unclassified.

By default, none of the classification rules are used. You need to enable them. Therefore, all unknown access points are categorized as Unclassified. When you create or change a rule, configure conditions and enable it, all rogue access points are then reclassified. Whenever you change a rule, it is applied to all access points (friendly, malicious, and unclassified) in the Alert state only.

If you move any rogue or ad hoc rogue manually to unclassified and Alert state, it means that the rogue is moved to the default state. Rogue rules apply to all the rogues that are manually moved to unclassified and Alert state.

Note Rule-based rogue classification does not apply to adhoc rogues and rogue clients.

Note You can configure up to 64 rogue classification rules per controller.

When the controller receives a rogue report from one of its managed access points, it responds as follows:

1. If the unknown access point is in the friendly MAC address list, the controller classifies the access point as Friendly.
2. If the unknown access point is not in the friendly MAC address list, the controller starts applying the rogue classification rules to the access point.
3. If the rogue is already classified as Malicious, Alert or Friendly, Internal or External, the controller does not reclassify it automatically. If the rogue is classified differently, the controller reclassifies it automatically only if the rogue is in the Alert state.
4. If the rogue access point matches the configured rules criteria, the controller classifies the rogue based on the classification type configured for that rule.
5. If the rogue access point does not match any of the configured rules, the rogue remains unclassified.

Note The controller repeats the previous steps for all the rogue access points.

6. If the rogue access point is detected on the same wired network, the controller marks the rogue state as Threat and classifies it as Malicious automatically, even if there are no configured rules. You can then manually contain the rogue to change the rogue state to Contained. If the rogue access point is not available on the network, the controller marks the rogue state as Alert. You can then manually contain the rogue.
7. If desired, you can manually move the access point to a different classification type and rogue state.

Table 83: Classification Mapping

Rule-Based Classification Type	Rogue States
Friendly	• Internal—If the unknown access point is inside the network and poses no threat to the WLAN security, you can manually configure it as Friendly, Internal. For instance, you can consider the access points in your lab network. • External—If the unknown access point is outside the network and poses no threat to WLAN security, you can manually configure it as Friendly, External. For instance, you can consider the access point in your neighboring coffee shop. • Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list.

Rule-Based Classification Type	Rogue States
Malicious	• Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list. • Threat—The unknown access point is found to be on the network and poses a threat to WLAN security. • Contained—The unknown access point is contained. • Contained Pending—The unknown access point is marked Contained, but the action is delayed due to unavailable resources.
Unclassified	• Pending—On first detection, the unknown access point is put in the Pending state for 3 minutes. During this time, the managed access points determine if the unknown access point is a neighbor access point. • Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list. • Contained—The unknown access point is contained. • Contained Pending—The unknown access point is marked Contained, but the action is delayed due to unavailable resources.

The classification and state of the rogue access points are configured as follows:

- From Known to Friendly, Internal
- From Acknowledged to Friendly, External
- From Contained to Malicious, Contained

As mentioned earlier, the controller can automatically change the classification type and rogue state of an unknown access point based on user-defined rules, or you can manually move the unknown access point to a different classification type and rogue state.

Table 84: Allowable Classification Type and Rogue State Transitions

From	To
Friendly (Internal, External, Alert)	Malicious (Alert)
Friendly (Internal, External, Alert)	Unclassified (Alert)
Friendly (Alert)	Friendly (Internal, External)
Malicious (Alert, Threat)	Friendly (Internal, External)
Malicious (Contained, Contained Pending)	Malicious (Alert)
Unclassified (Alert, Threat)	Friendly (Internal, External)
Unclassified (Contained, Contained Pending)	Unclassified (Alert)
Unclassified (Alert)	Malicious (Alert)

If the rogue state is Contained, you have to uncontain the rogue access point before you can change the classification type. If you want to move a rogue access point from Malicious to Unclassified, you must delete the access point and allow the controller to reclassify it.

Restrictions on Classifying Rogue Access Points

The following rules apply to this feature:

- Classifying Custom type rogues is tied to rogue rules. Therefore, it is not possible to manually classify a rogue as Custom. Custom class change can occur only using rogue rules.
- There are traps that are sent for containment by rule and every 30 minutes for rogue classification change. For custom classification, the first trap does not contain the severity score because the trap has existed before the custom classification. The severity score is obtained from the subsequent trap that is generated after 30 minutes if the rogue is classified.
- Rogue rules are applied on every incoming new rogue report in the controller in the order of their priority.
- Once a rogue satisfies a higher priority rule and is classified, it does not move down the priority list for the same report.
- Previously classified rogue gets re-classified on every new rogue report with the following restrictions:
  - Rogues which are classified as friendly by rule and whose state is set to ALERT, go through re-classification on receiving the new rogue report.
  - If a rogue is classified as friendly by the administrator manually, then the state is INTERNAL and it does not get re-classified on successive rogue reports.
  - If rogue is classified as malicious, irrespective of the state it does not get re-classified on subsequent rogue reports.
- Transition of the rogue's state from friendly to malicious is possible by multiple rogue rules if some attribute is missing in new rogue report.
- Transition of the rogue's state from malicious to any other classification is not possible by any rogue rule.
- The status change of a rogue device to contain or alert does not work when you move it between different class types until you move the class type of the rogue to unclassified.
- If a rogue AP is classified as friendly, it means that the rogue AP exists in the vicinity, is a known AP, and need not be tracked. Therefore, all the rogue clients are either deleted or not tracked if they are associated with the friendly rogue AP.
- When service set identifiers (SSIDs) are defined as part of a rogue rule, and details of the rogue rule are displayed using the **show wireless wps rogue rule detailed** command, the output differs in Cisco IOS XE Release 3.7E and prior releases and Cisco IOS XE Denali 16.1.1 and later releases.

  The following is sample output from the **show wireless wps rogue rule detailed** command in Cisco IOS XE Release 3.6E and prior releases:

```
Switch# show wireless wps rogue rule detailed test

Priority                                 : 1
Rule Name                                : wpstest
```

```
State                                    : Disabled
Type                                     : Pending
Match Operation                          : Any
Hit Count                                : 0
Total Conditions                         : 1
Condition :
  type                                   : Ssid
  SSID Count                             : 2
  SSID 1                                 : ssid1
  SSID 2                                 : ssid2
```

The following is sample output from the **show wireless wps rogue rule detailed** command in Cisco IOS XE Denali 16.1.1 and later releases:

```
Switch# show wireless wps rogue rule detailed test

Priority                                 : 1
Rule Name                                : wpstest
State                                    : Disabled
Type                                     : Pending
Match Operation                          : Any
Hit Count                                : 0
Total Conditions                         : 1
Condition :
  type                                   : Ssid
  SSID Count                             : 2
  SSID                                   : ssid1
  SSID                                   : ssid2
```

How to Classify Rogue Access Points

Configuring Rogue Classification Rules (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps rogue rule** *rule-name* **priority** *priority* **Example:** `Switch(config)# wireless wps rogue rule rule_3 priority 3`	Creates or enables a rule. While creating a rule, you must enter priority for the rule. **Note** After creating the rule, if you are editing the rule, you can change the priority only for the rogue rules that are disabled. You cannot change priority for the rogue rules that are enabled. While editing, changing the priority for a rogue rule is optional.

	Command or Action	Purpose

Step 3	**classify** {**friendly** | **malicious**}
	Example:
	`Switch(config)# wireless wps rogue rule rule_3 priority 3`
	`Switch(config-rule)# classify friendly`
		Classifies a rule.

Step 4	**condition** {**client-count** *condition_value* | **duration** | **encryption** | **infrastructure** | **rssi** | **ssid**}
	Example:
	`Switch(config)# wireless wps rogue rule rule_3 priority 3`
	`Switch(config-rule)# condition client-count 5`
		Specifies to add the following conditions to a rule that the rogue access point must meet:
		• **client-count**—Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point for the *condition_value* parameter. The valid range is 1 to 10 (inclusive), and the default value is 0.
		• **duration**—Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period for the *condition_value* parameter. The valid range is 0 to 3600 seconds (inclusive), and the default value is 0 seconds.
		• **encryption**—Requires that the advertised WLAN does not have encryption enabled.
		• **infrastructure**—Requires the SSID to be known to the controller.
		• **rssi**—Requires that the rogue access point have a minimum RSSI value. For example, if the rogue access point has an RSSI that is greater than the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value for the *condition_value parameter*. The valid range is –95 to –50 dBm (inclusive), and the default value is 0 dBm.
		• **ssid**—Requires that the rogue access point have a specific SSID. You should add SSIDs that are not managed by the

	Command or Action	Purpose
		controller. If you choose this option, enter the SSID for the *condition_value* parameter. The SSID is added to the user-configured SSID list.

Step 5	**match** {**all** | **any**}
	Example:
	`Switch(config)# wireless wps rogue rule rule_3 priority 3`
	`Switch(config-rule)# match all`
		Specifies whether a detected rogue access point must meet all or any of the conditions specified by the rule in order for the rule to be matched and the rogue access point to adopt the classification type of the rule.

Step 6	**default**
	Example:
	`Switch(config)# wireless wps rogue rule rule_3 priority 3`
	`Switch(config-rule)# default`
		Specifies to set a command to its default.

Step 7	**exit**
	Example:
	`Switch(config)# wireless wps rogue rule rule_3 priority 3`
	`Switch(config-rule)# exit`
	`Switch(config)#`
		Specifies to exit the sub-mode.

Step 8	**shutdown**
	Example:
	`Switch(config)# wireless wps rogue rule rule_3 priority 3`
	`Switch(config-rule)# shutdown`
		Specifies to disable a particular rogue rule. For example, the rule **rule_3** is disabled.

Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 10	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 11	**wireless wps rogue rule shutdown** **Example:** `Switch(config)# wireless wps rogue rule shutdown`	Specifies to disable all the rogue rules.

	Command or Action	Purpose
Step 12	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Rogue Classification Rules (GUI)

Procedure

Step 1 Choose **Security** > **Wireless Protection Policies** > **Rogue Policies** > **Rogue Rules** to open the Rogue Rules page.

Any rules that have already been created are listed in priority order. The name, type, and status of each rule is provided.

Note If you ever want to delete a rule, hover your mouse cursor over the blue drop-down arrow for that rule and click **Remove**.

Step 2 Create a new rule as follows:

a) Click **Add Rule**. An Add Rule section appears at the top of the page.

b) In the **Rule Name** text box, enter a name for the new rule. Ensure that the name does not contain any spaces.

c) From the **Rule Type** drop-down list, choose from the following options to classify rogue access points matching this rule as friendly or malicious:

- **Friendly**
- **Malicious**

d) Click **Add** to add this rule to the list of existing rules, or click **Cancel** to discard this new rule.

Step 3 Edit a rule as follows:

a) Click the name of the rule that you want to edit. The **Rogue Rule > Edit** page appears.

b) From the Type drop-down list, choose from the following options to classify rogue access points matching this rule:

- **Friendly**
- **Malicious**

c) From the Match Operation text box, choose one of the following:

All—If this rule is enabled, a detected rogue access point must meet all of the conditions specified by the rule in order for the rule to be matched and the rogue to adopt the classification type of the rule.

Any—If this rule is enabled, a detected rogue access point must meet any of the conditions specified by the rule in order for the rule to be matched and the rogue to adopt the classification type of the rule. This is the default value.

d) To enable this rule, select the **Enable Rule** check box. The default value is unselected.

e) To disable this particular rule, unselect the **Enable Rule** check box.

Note You cannot disable all the rogue rule in one shot from GUI but you can disable all the rogue rules from CLI using the **wireless wps rogue rule shutdown** command.

f) From the Add Condition drop-down list, choose one or more of the following conditions that the rogue access point must meet and click **Add Condition**.

- **SSID**—Requires that the rogue access point have a specific user-configured SSID. If you choose this option, enter the SSID in the User Configured SSID text box, and click **Add SSID**. The user-configured SSIDs are added and listed.

  Note To delete an SSID, highlight the SSID and click **Remove**. The SSID applied on a WLAN cannot be applied for the rogue rule.

- **RSSI**—Requires that the rogue access point have a minimum Received Signal Strength Indication (RSSI) value. For example, if the rogue access point has an RSSI that is greater than the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value in the Minimum RSSI text box. The valid range is –95 to –50 dBm (inclusive), and the default value is 0 dBm.
- **Duration**—Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period in the Time Duration text box. The valid range is 0 to 3600 seconds (inclusive), and the default value is 0 seconds.
- **Client Count**—Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point in the Minimum Number of Rogue Clients text box. The valid range is 1 to 10 (inclusive), and the default value is 0.
- **No Encryption**—Requires that the rogue access point's advertised WLAN does not have encryption enabled. If a rogue access point has encryption disabled, it is likely that more clients will try to associate to it. No further configuration is required for this option.

  Note Cisco Prime Infrastructure refers to this option as "Open Authentication."

- **Managed SSID**—Requires that the rogue access point's managed SSID (the SSID configured for the WLAN) be known to the controller. No further configuration is required for this option.

  Note The SSID and Managed SSID conditions cannot be used with the All operation because these two SSID lists are mutually exclusive. If you define a rule with Match All and have these two conditions configured, the rogue access points are never classified as friendly or malicious because one of the conditions can never be met.

  You can add up to six conditions per rule. When you add a condition, it appears under the Conditions section.

  Note If you ever want to delete a condition from this rule, click **Remove** near the condition.

- **User configured SSID**—Requires that the rogue access point have a substring of the specific user-configured SSID. The controller searches the substring in the same occurrence pattern and returns a match if the substring is found in the whole string of an SSID.

g) Click **Apply**.

Step 4 If you want to change the priority in which rogue classification rules are applied, follow these steps:

1. Click **Change Priority** to access the Rogue Rules > Priority page.

   The rogue rules are listed in priority order in the Change Rules Priority text box.

2. Click on a specific rule for which you want to change the priority, and click **Up** to raise its priority in the list or **Down** to lower its priority in the list.

   Note You can change priority only for the disabled rule. You cannot change priority only for the enabled rule.

3. Click **Apply**.

Viewing and Classifying Rogue Devices (GUI)

Procedure

Step 1 Choose **Monitor** > **Rogues**.

Step 2 Choose the following options to view the different types of rogue access points detected by the controller:

- **Friendly APs**
- **Malicious APs**
- **Unclassified APs**

The respective rogue APs pages provide the following information: the MAC address of the rogue access point, the number of radios that detected the rogue access point, the number of clients connected to the rogue access point, the current status of the rogue access point, and last heard.

Step 3 Get more details about a rogue access point by clicking the MAC address of the access point. The Rogue AP Detail page appears.

This page provides the following information: the MAC address of the rogue device, the type of rogue device (such as an access point), whether the rogue device is on the wired network, the dates and times when the rogue device was first and last reported, and the current status of the device.

The Class Type text box shows the current classification for this rogue access point:

- **Friendly**—An unknown access point that matches the user-defined friendly rules or an existing known and acknowledged rogue access point. Friendly access points cannot be contained.
- **Malicious**—An unknown access point that matches the user-defined malicious rules or is moved manually by the user from the Friendly or Unclassified classification type.

  Note Once an access point is classified as Malicious, you cannot apply rules to it in the future, and it cannot be moved to another classification type. If you want to move a malicious access point to the Unclassified classification type, you must delete the access point and allow the controller to reclassify it.

- **Unclassified**—An unknown access point that does not match the user-defined friendly or malicious rules. An unclassified access point can be contained. It can also be moved to the Friendly or Malicious classification type automatically in accordance with user-defined rules or manually by the user.

Step 4 If you want to change the classification of this device, choose a different classification from the Class Type drop-down list.

Note A rogue access point cannot be moved to another class if its current state is Contain.

Step 5 From the Update Status drop-down list, choose one of the following options to specify how the controller should respond to this rogue access point:

- **Internal**—The controller trusts this rogue access point. This option is available if the Class Type is set to Friendly.
- **External**—The controller acknowledges the presence of this rogue access point. This option is available if the Class Type is set to Friendly.
- **Contain**—The controller contains the offending device so that its signals no longer interfere with authorized clients. This option is available if the Class Type is set to Malicious or Unclassified.
- **Alert**—The controller forwards an immediate alert to the system administrator for further action. This option is available if the Class Type is set to Malicious or Unclassified.

The bottom of the page provides information on both the access points that detected this rogue access point and any clients that are associated to it. To see more details for any of the clients, click **Edit** to open the Rogue Client Detail page.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Step 8 See any adhoc rogues detected by the controller by choosing **Adhoc Rogues**. The Adhoc Rogues page appears.

This page shows the following information: the MAC address, BSSID, and SSID of the adhoc rogue, the number of radios that detected the adhoc rogue, and the current status of the adhoc rogue.

Step 9 Obtain more details about an adhoc rogue by clicking the MAC address of the rogue. The Adhoc Rogue Detail page appears.

This page provides the following information: the MAC address and BSSID of the adhoc rogue, the dates and times when the rogue was first and last reported, and the current status of the rogue.

Step 10 From the Update Status drop-down list, choose one of the following options to specify how the controller should respond to this adhoc rogue:

- **Contain**—The controller contains the offending device so that its signals no longer interfere with authorized clients.
- **Alert**—The controller forwards an immediate alert to the system administrator for further action.
- **Internal**—The controller trusts this rogue access point.
- **External**—The controller acknowledges the presence of this rogue access point.

Step 11 From the Maximum Number of APs to Contain the Rogue drop-down list, choose one of the following options to specify the maximum number of access points used to contain this adhoc rogue: **1**, **2**, **3**, or **4**.

The bottom of the page provides information on the access points that detected this adhoc rogue.

Step 12 Click **Apply**.

Step 13 Click **Save Configuration**.

Step 14 View any access points that have been configured to be ignored by choosing **Rogue AP Ignore-List**. The Rogue AP Ignore-List page appears.

This page shows the MAC addresses of any access points that are configured to be ignored. The rogue-ignore list contains a list of any autonomous access points that have been manually added to Cisco Prime Infrastructure maps by the users. The controller regards these autonomous access points as rogues even though the Prime Infrastructure is managing them. The rogue-ignore list allows the controller to ignore these access points. The list is updated as follows:

- When the controller receives a rogue report, it checks to see if the unknown access point is in the rogue-ignore access point list.
- If the unknown access point is in the rogue-ignore list, the controller ignores this access point and continues to process other rogue access points.
- If the unknown access point is not in the rogue-ignore list, the controller sends a trap to the Prime Infrastructure. If the Prime Infrastructure finds this access point in its autonomous access point list, the Prime Infrastructure sends a command to the controller to add this access point to the rogue-ignore list. This access point is then ignored in future rogue reports.
- If a user removes an autonomous access point from the Prime Infrastructure, the Prime Infrastructure sends a command to the controller to remove this access point from the rogue-ignore list.

Examples: Classifying Rogue Access Points

This example shows how to create a rule that can organize and display rogue access points as Friendly:

```
Switch# configure terminal
Switch(config)# wireless wps rogue rule ap1 priority 1
Switch(config-rule)# classify friendly
Switch(config-rule)# end
```

This example shows how to apply condition that the rogue access point must meet:

```
Switch# configure terminal
Switch(config)# wireless wps rogue rule ap1 priority 1
Switch(config-rule)# condition client-count 5
Switch(config-rule)# condition duration 1000
Switch(config-rule)# end
```

Additional References for Classifying Rogue Access Points

Related Documents

Related Topic	Document Title
Security commands	*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

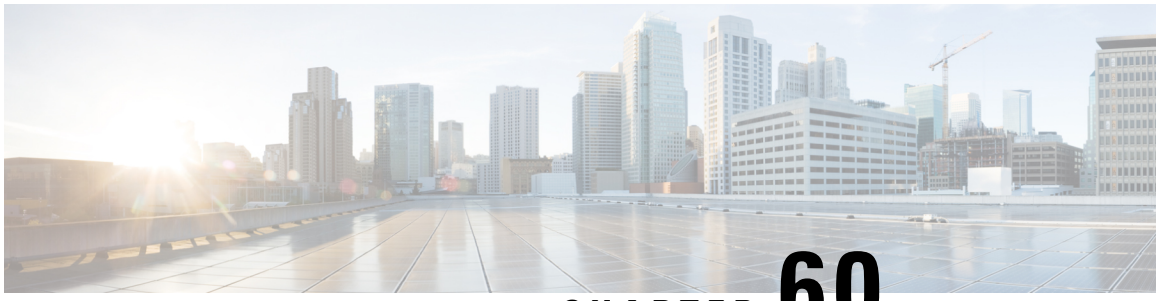
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Classifying Rogue Access Points

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.



CHAPTER 60

Configuring wIPS

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About wIPS

The Cisco Adaptive Wireless Intrusion Prevention System (wIPS) uses an advanced approach to wireless threat detection and performance management. It combines network traffic analysis, network device and topology information, signature-based techniques, and anomaly detection to deliver highly accurate and complete wireless threat prevention. With a fully infrastructure-integrated solution, you can continually monitor wireless traffic on both the wired and wireless networks and use that network intelligence to analyze attacks from many sources to accurately pinpoint and proactively prevent attacks, rather than wait until damage or exposure has occurred.

Cisco Adaptive wIPS is a part of the Cisco 3300 Series Mobility Services Engine (MSE), which centralizes the processing of intelligence collected by the continuous monitoring of Cisco Aironet APs. With Cisco Adaptive wIPS functionalities and Cisco Prime Infrastructure integration into the Cisco MSE, the wIPS can configure and monitor wIPS policies and alarms and report threats.

Note If your wIPS deployment consists of a Cisco WLC, access point, and Cisco MSE, you must set all the three entities to the UTC time zone.

Cisco Adaptive wIPS is not configured on the Cisco WLC. Instead, the Cisco Prime Infrastructure forwards the profile configuration to the wIPS service, which forwards the profile to the Cisco WLC. The profile is stored in flash memory on the Cisco WLC and sent to APs when they join the Cisco WLC. When an access point disassociates and joins another Cisco WLC, it receives the wIPS profile from the new Cisco WLC.

Local-mode APs with a subset of wIPS capabilities are referred to as Enhanced Local Mode access point or ELM AP. You can configure an access point to work in the wIPS mode if the AP is in any of the following modes:

- Monitor
- Local

The regular local mode AP is extended with a subset of wIPS capabilities. This feature enables you to deploy your APs to provide protection without needing a separate overlay network.

wIPS ELM has the limited capability of detecting off-channel alarms. AN AP periodically goes off-channel, and monitors the nonserving channels for a short duration, and triggers alarms if any attack is detected on the channel. But off-channel alarm detection is best effort, and it takes a longer time to detect attacks and trigger alarms, which might cause the ELM AP to intermittently detect an alarm and clear it because it is not visible. APs in any of the above modes can periodically send alarms based on the policy profile to the wIPS service through the Cisco WLC. The wIPS service stores and processes the alarms and generates SNMP traps. Cisco Prime Infrastructure configures its IP address as a trap destination to receive SNMP traps from the Cisco MSE.

This table lists all the SNMP trap controls and their respective traps. When a trap control is enabled, all the traps of that trap control are also enabled.

Note The Cisco WLC uses only SNMPv2 for SNMP trap transmission.

Table 85: SNMP Trap Controls and Their Respective Traps

Tab Name	Trap Control	Trap
General	Link (Port) Up/Down	linkUp, linkDown
	Spanning Tree	newRoot, topologyChange, stpInstanceNewRootTrap, stpInstanceTopologyChangeTrap
	Config Save	bsnDot11EssCreated, bsnDot11EssDeleted, bsnConfigSaved, ciscoLwappScheduledResetNotif, ciscoLwappClearResetNotif, ciscoLwappResetFailedNotif, ciscoLwappSysInvalidXmlConfig

Tab Name	Trap Control	Trap
AP	AP Register	bsnAPDisassociated, bsnAPAssociated
	AP Interface Up/Down	bsnAPIfUp, bsnAPIfDown
Client Traps	802.11 Association	bsnDot11StationAssociate
	802.11 Disassociation	bsnDot11StationDisassociate
	802.11 Deauthentication	bsnDot11StationDeauthenticate
	802.11 Failed Authentication	bsnDot11StationAuthenticateFail
	802.11 Failed Association	bsnDot11StationAssociateFail
	Exclusion	bsnDot11StationBlacklisted
	NAC Alert	cldcClientWlanProfileName, cldcClientIPAddress, cldcApMacAddress, cldcClientQuarantineVLAN, cldcClientAccessVLAN
Security Traps	User Authentication	bsnTooManyUnsuccessLoginAttempts, cLWAGuestUserLoggedIn, cLWAGuestUserLoggedOut
	RADIUS Servers Not Responding	bsnRADIUSServerNotResponding, ciscoLwappAAARadiusReqTimedOut
	WEP Decrypt Error	bsnWepKeyDecryptError
	Rogue AP	bsnAdhocRogueAutoContained, bsnRogueApAutoContained, bsnTrustedApHasInvalidEncryption, bsnMaxRogueCountExceeded, bsnMaxRogueCountClear, bsnApMaxRogueCountExceeded, bsnApMaxRogueCountClear, bsnTrustedApHasInvalidRadioPolicy, bsnTrustedApHasInvalidSsid, bsnTrustedApIsMissing
	SNMP Authentication	agentSnmpAuthenticationTrapFlag
	Multiple Users	multipleUsersTrap

Tab Name	Trap Control	Trap
Auto RF Profile Traps	Load Profile	bsnAPLoadProfileFailed
	Noise Profile	bsnAPNoiseProfileFailed
	Interference Profile	bsnAPInterferenceProfileFailed
	Coverage Profile	bsnAPCoverageProfileFailed
Auto RF Update Traps	Channel Update	bsnAPCurrentChannelChanged
	Tx Power Update	bsnAPCurrentTxPowerChanged
Mesh Traps	Child Excluded Parent	ciscoLwappMeshChildExcludedParent
	Parent Change	ciscoLwappMeshParentChange
	Authfailure Mesh	ciscoLwappMeshAuthorizationFailure
	Child Moved	ciscoLwappMeshChildMoved
	Excessive Parent Change	ciscoLwappMeshExcessiveParentChange
	Excessive Children	ciscoLwappMeshExcessiveChildren
	Poor SNR	ciscoLwappMeshAbateSNR, ciscoLwappMeshOnsetSNR
	Console Login	ciscoLwappMeshConsoleLogin
	Excessive Association	ciscoLwappMeshExcessiveAssociation
	Default Bridge Group Name	ciscoLwappMeshDefaultBridgeGroupName

The following are the trap descriptions for the traps mentioned in the *SNMP Trap Controls and Their Respective Traps* table:

- General Traps
  - SNMP Authentication—The SNMPv2 entity has received a protocol message that is not properly authenticated.

Note When a user who is configured in SNMP V3 mode tries to access the Cisco WLC with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.

  - Link (Port) Up/Down—Link changes status from up or down.
  - Link (Port) Up/Down—Link changes status from up or down.
  - Multiple Users—Two users log in with the same ID.
  - Rogue AP—Whenever a rogue access point is detected, this trap is sent with its MAC address; when a rogue access point that was detected earlier no longer exists, this trap is sent.
  - Config Save—Notification that is sent when the Cisco WLC configuration is modified.

- Cisco AP Traps
  - AP Register—Notification sent when an access point associates or disassociates with the Cisco WLC.
  - AP Interface Up/Down—Notification sent when an access point interface (802.11X) status goes up or down.
- Client-Related Traps
  - 802.11 Association—Associate notification that is sent when a client sends an association frame.
  - 802.11 Disassociation—Disassociate notification that is sent when a client sends a disassociation frame.
  - 802.11 Deauthentication—Deauthenticate notification that is sent when a client sends a deauthentication frame.
  - 802.11 Failed Authentication—Authenticate failure notification that is sent when a client sends an authentication frame with a status code other than successful.
  - 802.11 Failed Association—Associate failure notification that is sent when the client sends an association frame with a status code other than successful.
  - Exclusion—Associate failure notification that is sent when a client is exclusion listed (blacklisted).

Note The maximum number of static blacklist entries that the APs can have is 340.

  - Authentication—Authentication notification that is sent when a client is successfully authenticated.
  - Max Clients Limit Reached—Notification that is sent when the maximum number of clients, defined in the Threshold field, are associated with the Cisco WLC.
  - NAC Alert—Alert that is sent when a client joins an SNMP NAC-enabled WLAN.

    This notification is generated when a client on NAC-enabled SSIDs completes Layer2 authentication to inform the NAC appliance about the client's presence. cldcClientWlanProfileName represents the profile name of the WLAN that the 802.11 wireless client is connected to, cldcClientIPAddress represents the unique IP address of the client. cldcApMacAddress represents the MAC address of the AP to which the client is associated. cldcClientQuarantineVLAN represents the quarantine VLAN for the client. cldcClientAccessVLAN represents the access VLAN for the client.
  - Association with Stats—Associate notification that is sent with data statistics when a client is associated with the Cisco WLC, or roams. Data statistics include transmitted and received bytes and packets.
  - Disassociation with Stats—Disassociate notification that is sent with data statistics when a client disassociates from the Cisco WLC. Data statistics include transmitted and received bytes and packets, SSID, and session ID.

Note When you downgrade to Release 7.4 from a later release, if a trap that was not supported in Release 7.4 (for example, NAC Alert trap) is enabled before the downgrade, all traps are disabled. After the downgrade, you must enable all the traps that were enabled before the downgrade. We recommend that you disable the new traps before the downgrade so that all the other traps are not disabled.

- Security Traps
  - User Auth Failure—This trap informs that a client RADIUS Authentication failure has occurred.
  - RADIUS Server No Response—This trap is to indicate that no RADIUS servers are responding to authentication requests sent by the RADIUS client.
  - WEP Decrypt Error—Notification sent when the Cisco WLC detects a WEP decrypting error.
  - Rouge AP—Whenever a rogue access point is detected, this trap is sent with its MAC address; when a rogue access point that was detected earlier no longer exists, this trap is sent.
  - SNMP Authentication—The SNMPv2 entity has received a protocol message that is not properly authenticated.

Note When a user who is configured in SNMP V3 mode tries to access the Cisco WLC with an incorrect password, authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.

  - Multiple Users—Two users log in with the same ID.
- SNMP Authentication
  - Load Profile—Notification sent when the Load Profile state changes between PASS and FAIL.
  - Noise Profile—Notification sent when the Noise Profile state changes between PASS and FAIL.
  - Interference Profile—Notification sent when the Interference Profile state changes between PASS and FAIL.
  - Coverage Profile—Notification sent when the Coverage Profile state changes between PASS and FAIL.
- Auto RF Profile Traps
  - Load Profile—Notification sent when the Load Profile state changes between PASS and FAIL.
  - Noise Profile—Notification sent when the Noise Profile state changes between PASS and FAIL.
  - Interference Profile—Notification sent when the Interference Profile state changes between PASS and FAIL.
  - Coverage Profile—Notification sent when the Coverage Profile state changes between PASS and FAIL.
- Auto RF Update Traps
  - Channel Update—Notification sent when the access point dynamic channel algorithm is updated.
  - Tx Power Update—Notification sent when the access point dynamic transmit power algorithm is updated.
- Mesh Traps
  - Child Excluded Parent—Notification that is sent when a defined number of failed association to the Cisco WLC occurs through a parent mesh node.
  - Notification sent when a child mesh node exceeds the threshold limit of the number of discovery response timeouts. The child mesh node does not try to associate an excluded parent mesh node for the interval defined. The child mesh node remembers the excluded parent MAC address when it joins the network, and informs the Cisco WLC.
  - Parent Change—Notification is sent by the agent when a child mesh node changes its parent. The child mesh node remembers previous parent and informs the Cisco WLC about the change of parent when it rejoins the network.

- Child Moved—Notification sent when a parent mesh node loses connection with its child mesh node.
- Excessive Parent Change—Notification sent when the child mesh node changes its parent frequently. Each mesh node keeps a count of the number of parent changes in a fixed time. If it exceeds the defined threshold, the child mesh node informs the Cisco WLC.
- Excessive Children—Notification sent when the child count exceeds for a RAP and a MAP.
- Poor SNR—Notification sent when the child mesh node detects a lower SNR on a backhaul link. For the other trap, a notification is sent to clear a notification when the child mesh node detects an SNR on a backhaul link that is higher then the object defined by 'clMeshSNRThresholdAbate'.
- Console Login—Notification is sent by the agent when a login on a MAP console is either successful or fail after three attempts.
- Default Bridge Group Name—Notification sent when the MAP mesh node joins its parent using the default bridge group name.

Note The remaining traps do not have trap controls. These traps are not generated too frequently and do not require any trap control. Any other trap that is generated by the Cisco WLC cannot be turned off.

Note In all of the above cases, the Cisco WLC functions solely as a forwarding device.

How to Configure wIPS on an Access Point

Configuring wIPS on an Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap name** *name* **mode** *submode wips* **Example:** `Switch# ap name ap1 mode local wips`	Configure an access point for local or monitor mode and then set the submode to wIPS.
Step 2	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 3	**show wireless wps wips summary** **Example:** `Switch# show wireless wps wips summary`	View the wIPS configuration on the access point.
Step 4	**show wireless wps wips statistics** **Example:**	View the current state of wIPS configuration.

	Command or Action	Purpose
	`Switch# show wireless wps wips statistics`	

Configuring wIPS on an Access Point (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points** > **All APs**.

The **All APs** page appears with a list of all access points that are associated with the switch.

Step 2 Click the name of the access point for which you want to configure wIPS.

The **AP** > **Edit** page appears.

Step 3 In the General area, set the **AP Mode** parameter. To configure an access point for wIPS, you must choose one of the following modes from the **AP Mode** drop-down list:

- **Local**
- **Monitor**

Step 4 Set the **AP Sub Mode** to wIPS by choosing **wIPS** from the **AP Sub Mode** drop-down list.

Step 5 Click **Apply**.

Step 6 Click **Save**.

Monitoring wIPS Information

This section describes the new command for wIPS.

The following command can be used to monitor wIPS configured on the access point.

Table 86: Monitoring wIPS Command

Command	Purpose
show wireless wps wips summary	Displays the wIPS configuration on the access point.
show wireless wps wips statistics	Displays the current state of wIPS configuration.

Examples: wIPS Configuration

This example shows how to configure wIPS on AP1:

```
Switch# ap name ap1 mode local submode wips
Switch# end
Switch# show wireless wps wips summary
```

Additional References for Configuring wIPS

Related Documents

Related Topic	Document Title
wIPS commands	*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

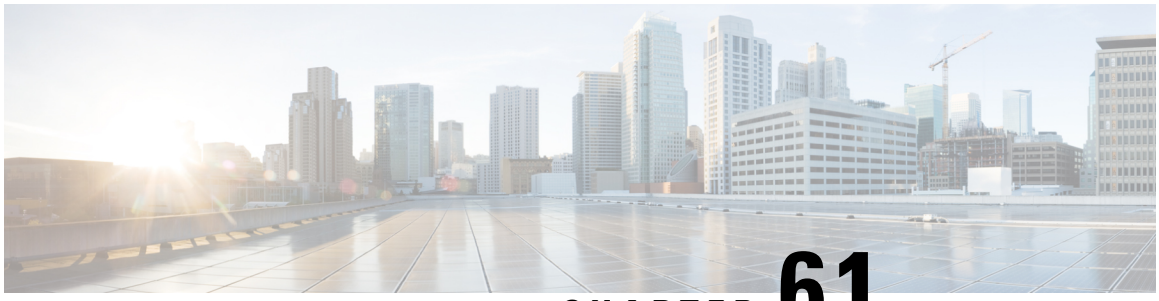
Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History for Performing wIPS Configuration

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.

PART XII

System Management



CHAPTER 61

Administering the System

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Administering the Switch

System Time and Date Management

You can manage the system time and date on your switch using automatic configuration methods (RTC and NTP), or manual configuration methods.

Note For complete syntax and usage information for the commands used in this section, see the *Cisco IOS Configuration Fundamentals Command Reference*on *Cisco.com*.

System Clock

The basis of the time service is the system clock. This clock runs from the moment the system starts up and keeps track of the date and time.

The system clock can then be set from these sources:

- NTP
- Manual configuration

The system clock can provide time to these services:

- User **show** commands
- Logging and debugging messages

The system clock keeps track of time internally based on Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT). You can configure information about the local time zone and summer time (daylight saving time) so that the time appears correctly for the local time zone.

The system clock keeps track of whether the time is *authoritative* or not (that is, whether it has been set by a time source considered to be authoritative). If it is not authoritative, the time is available only for display purposes and is not redistributed.

Network Time Protocol

The NTP is designed to time-synchronize a network of devices. NTP runs over User Datagram Protocol (UDP), which runs over IP. NTP is documented in RFC 1305.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

NTP uses the concept of a *stratum* to describe how many NTP hops away a device is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached, a stratum 2 time server receives its time through NTP from a stratum 1 time server, and so on. A device running NTP automatically chooses as its time source the device with the lowest stratum number with which it communicates through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP avoids synchronizing to a device whose time might not be accurate by never synchronizing to a device that is not synchronized. NTP also compares the time reported by several devices and does not synchronize to a device whose time is significantly different than the others, even if its stratum is lower.

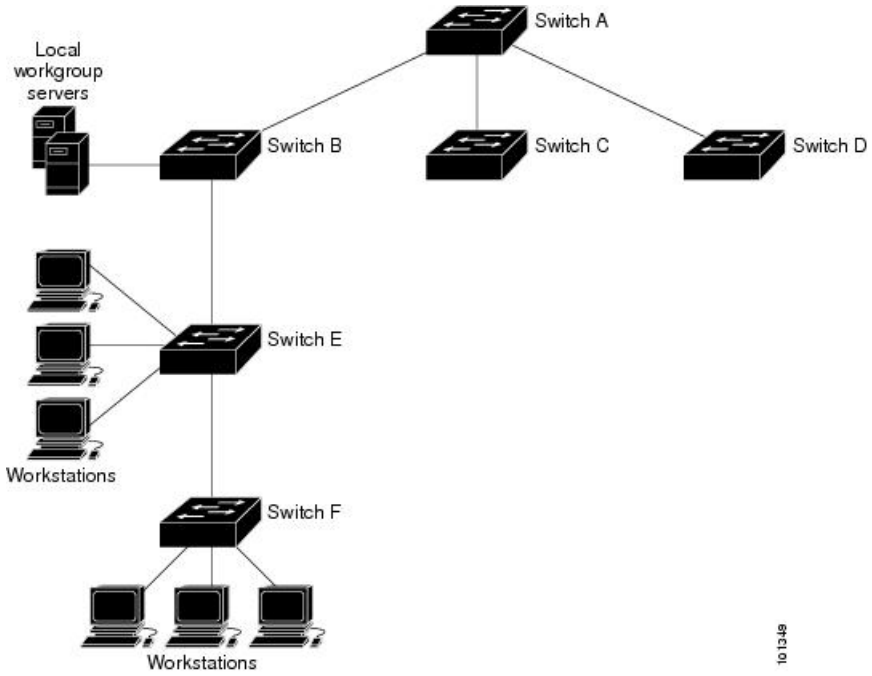
The communications between devices running NTP (known as associations) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, in that case, information flow is one-way only.

The time kept on a device is a critical resource; you should use the security features of NTP to avoid the accidental or malicious setting of an incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.

Cisco's implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that the time service for your network be derived from the public NTP servers available on the IP Internet.

The figure below shows a typical network example using NTP. Switch A is the NTP master, with the **Switch** B, C, and D configured in NTP server mode, in server association with Switch A. Switch E is configured as an NTP peer to the upstream and downstream Switch, Switch B and Switch F, respectively.

Figure 69: Typical NTP Network Configuration



If the network is isolated from the Internet, Cisco's implementation of NTP allows a device to act as if it is synchronized through NTP, when in fact it has learned the time by using other means. Other devices then synchronize to that device through NTP.

When multiple sources of time are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

Several manufacturers include NTP software for their host systems, and a publicly available version for systems running UNIX and its various derivatives is also available. This software allows host systems to be time-synchronized as well.

NTP Stratum

NTP uses the concept of a *stratum* to describe how many NTP hops away a device is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached, a stratum 2 time server receives its time through NTP from a stratum 1 time server, and so on. A device running NTP automatically chooses as its time source the device with the lowest stratum number with which it communicates through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP avoids synchronizing to a device whose time might not be accurate by never synchronizing to a device that is not synchronized. NTP also compares the time reported by several devices and does not synchronize to a device whose time is significantly different than the others, even if its stratum is lower.

NTP Associations

The communications between devices running NTP (known as *associations*) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, in that case, information flow is one-way only.

NTP Security

The time kept on a device is a critical resource; you should use the security features of NTP to avoid the accidental or malicious setting of an incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.

NTP Implementation

Implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that the time service for your network be derived from the public NTP servers available on the IP Internet.

If the network is isolated from the Internet, NTP allows a device to act as if it is synchronized through NTP, when in fact it has learned the time by using other means. Other devices then synchronize to that device through NTP.

When multiple sources of time are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

Several manufacturers include NTP software for their host systems, and a publicly available version for systems running UNIX and its various derivatives is also available. This software allows host systems to be time-synchronized as well.

NTP Version 4

NTP version 4 is implemented on the switch. NTPv4 is an extension of NTP version 3. NTPv4 supports both IPv4 and IPv6 and is backward-compatible with NTPv3.

NTPv4 provides these capabilities:

- Support for IPv6.
- Improved security compared to NTPv3. The NTPv4 protocol provides a security framework based on public key cryptography and standard X509 certificates.
- Automatic calculation of the time-distribution hierarchy for a network. Using specific multicast groups, NTPv4 automatically configures the hierarchy of the servers to achieve the best time accuracy for the lowest bandwidth cost. This feature leverages site-local IPv6 multicast addresses.

For details about configuring NTPv4, see the *Implementing NTPv4 in IPv6* chapter of the *Cisco IOS IPv6 Configuration Guide, Release 12.4T*.

DNS

The DNS protocol controls the Domain Name System (DNS), a distributed database with which you can map hostnames to IP addresses. When you configure DNS on your switch, you can substitute the hostname for the IP address with all IP commands, such as **ping**, **telnet**, **connect**, and related Telnet support operations.

IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, for example, the File Transfer Protocol (FTP) system is identified as *ftp.cisco.com*.

To keep track of domain names, IP has defined the concept of a domain name server, which holds a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the hostnames, specify the name server that is present on your network, and enable the DNS.

Default DNS Settings

Table 87: Default DNS Settings

Feature	Default Setting
DNS enable state	Enabled.
DNS default domain name	None configured.
DNS servers	No name server addresses are configured.

Login Banners

You can configure a message-of-the-day (MOTD) and a login banner. The MOTD banner is displayed on all connected terminals at login and is useful for sending messages that affect all network users (such as impending system shutdowns).

The login banner is also displayed on all connected terminals. It appears after the MOTD banner and before the login prompts.

Note For complete syntax and usage information for the commands used in this section, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.4*.

Default Banner Configuration

The MOTD and login banners are not configured.

MAC Address Table

The MAC address table contains address information that the switch uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports. The address table includes these types of addresses:

- Dynamic address—A source MAC address that the switch learns and then ages when it is not in use.

- Static address—A manually entered unicast address that does not age and that is not lost when the switch resets.

The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address and the type (static or dynamic).

Note For complete syntax and usage information for the commands used in this section, see the command reference for this release.

MAC Address Table Creation

With multiple MAC addresses supported on all ports, you can connect any port on the switch to other network devices. The switch provides dynamic addressing by learning the source address of packets it receives on each port and adding the address and its associated port number to the address table. As devices are added or removed from the network, the switch updates the address table, adding new dynamic addresses and aging out those that are not in use.

The aging interval is globally configured. However, the switch maintains an address table for each VLAN, and STP can accelerate the aging interval on a per-VLAN basis.

The switch sends packets between any combination of ports, based on the destination address of the received packet. Using the MAC address table, the switch forwards the packet only to the port associated with the destination address. If the destination address is on the port that sent the packet, the packet is filtered and not forwarded. The switch always uses the store-and-forward method: complete packets are stored and checked for errors before transmission.

MAC Addresses and VLANs

All addresses are associated with a VLAN. An address can exist in more than one VLAN and have different destinations in each. Unicast addresses, for example, could be forwarded to port 1 in VLAN 1 and ports 9, 10, and 1 in VLAN 5.

Each VLAN maintains its own logical address table. A known address in one VLAN is unknown in another until it is learned or statically associated with a port in the other VLAN.

Default MAC Address Table Settings

The following table shows the default settings for the MAC address table.

Table 88: Default Settings for the MAC Address

Feature	Default Setting
Aging time	300 seconds
Dynamic addresses	Automatically learned
Static addresses	None configured

ARP Table Management

To communicate with a device (over Ethernet, for example), the software first must learn the 48-bit MAC address or the local data link address of that device. The process of learning the local data link address from an IP address is called *address resolution*.

The Address Resolution Protocol (ARP) associates a host IP address with the corresponding media or MAC addresses and the VLAN ID. Using an IP address, ARP finds the associated MAC address. When a MAC address is found, the IP-MAC address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network. Encapsulation of IP datagrams and ARP requests and replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP). By default, standard Ethernet-style ARP encapsulation (represented by the **arpa** keyword) is enabled on the IP interface.

ARP entries added manually to the table do not age and must be manually removed.

For CLI procedures, see the Cisco IOS Release 12.4 documentation on *Cisco.com*.

How to Administer the Switch

Configuring the Time and Date Manually

System time remains accurate through restarts and reboot, however, you can manually configure the time and date after the system is restarted.

We recommend that you use manual configuration only when necessary. If you have an outside source to which the switch can synchronize, you do not need to manually set the system clock.

Setting the System Clock

If you have an outside source on the network that provides time services, such as an NTP server, you do not need to manually set the system clock.

Follow these steps to set the system clock:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	Use one of the following: • **clock set** *hh:mm:ss day month year* • **clock set** *hh:mm:ss month day year* **Example:**	Manually set the system clock using one of these formats: • *hh:mm:ss*—Specifies the time in hours (24-hour format), minutes, and seconds. The time specified is relative to the configured time zone.

	Command or Action	Purpose
	`Switch# clock set 13:32:00 23 March 2013`	• *day*—Specifies the day by date in the month. • *month*—Specifies the month by name. • *year*—Specifies the year (no abbreviation).

Configuring the Time Zone

Follow these steps to manually configure the time zone:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**clock timezone** *zone hours-offset* [*minutes-offset*] **Example:** `Switch(config)# clock timezone AST -3 30`	Sets the time zone. Internal time is kept in Coordinated Universal Time (UTC), so this command is used only for display purposes and when the time is manually set. • *zone*—Enters the name of the time zone to be displayed when standard time is in effect. The default is UTC. • *hours-offset*—Enters the hours offset from UTC. • (Optional) *minutes-offset*—Enters the minutes offset from UTC. This available where the local time zone is a percentage of an hour different from UTC.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Summer Time (Daylight Saving Time)

To configure summer time (daylight saving time) in areas where it starts and ends on a particular day of the week each year, perform this task:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

Step 3	**clock summer-time** *zone* **date** *date month year hh:mm date month year hh:mm* [*offset*]]
	Example:
	`Switch(config)# clock summer-time PDT date`
	`10 March 2013 2:00 3 November 2013 2:00`
		Configures summer time to start and end on specified days every year.

Step 4	**clock summer-time** *zone* **recurring** [*week day month hh:mm week day month hh:mm* [*offset*]] **Example:** `Switch(config)# clock summer-time PDT recurring 10 March 2013 2:00 3`	Configures summer time to start and end on the specified days every year. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. Summer time is disabled by default. If you

	Command or Action	Purpose
	`November 2013 2:00`	specify **clock summer-time** *zone* **recurring** without parameters, the summer time rules default to the United States rules. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere. • *zone*—Specifies the name of the time zone (for example, PDT) to be displayed when summer time is in effect. • (Optional) *week*— Specifies the week of the month (1 to 4, **first**, or **last**). • (Optional) *day*—Specifies the day of the week (Sunday, Monday...). • (Optional) *month*—Specifies the month (January, February...). • (Optional) *hh:mm*—Specifies the time (24-hour format) in hours and minutes. • (Optional) *offset*—Specifies the number of minutes to add during summer time. The default is 60.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Follow these steps if summer time in your area does not follow a recurring pattern (configure the exact date and time of the next summer time events):

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**clock summer-time** *zone* **date**[*month date year hh:mm month date year hh:mm* [*offset*]]or**clock summer-time** *zone* **date** [*date month year hh:mm date month year hh:mm* [*offset*]]	Configures summer time to start on the first date and end on the second date. Summer time is disabled by default. • For *zone*, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect. • (Optional) For *week*, specify the week of the month (1 to 5 or last). • (Optional) For *day*, specify the day of the week (Sunday, Monday...). • (Optional) For *month*, specify the month (January, February...). • (Optional) For *hh:mm*, specify the time (24-hour format) in hours and minutes. • (Optional) For *offset*, specify the number of minutes to add during summer time. The default is 60.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.

	Command or Action	Purpose
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring a System Name

Follow these steps to manually configure a system name:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**hostname** *name* **Example:** `Switch(config)# hostname remote-users`	Configures a system name. When you set the system name, it is also used as the system prompt. The default setting is Switch. The name must follow the rules for ARPANET hostnames. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names can be up to 63 characters.

Step 4	**end**
	Example:
	`remote-users(config)#end`
	`remote-users#`
		Returns to priviliged EXEC mode.

Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.

	Command or Action	Purpose
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Setting Up DNS

If you use the switch IP address as its hostname, the IP address is used and no DNS query occurs. If you configure a hostname that contains no periods (.), a period followed by the default domain name is appended to the hostname before the DNS query is made to map the name to an IP address. The default domain name is the value set by the **ip domain-name** global configuration command. If there is a period (.) in the hostname, the Cisco IOS software looks up the IP address without appending any default domain name to the hostname.

Follow these steps to set up your switch to use the DNS:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip domain-name** *name* **Example:** `Switch(config)# ip domain-name Cisco.com`	Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name. At boot time, no domain name is configured; however, if the switch configuration comes from a BOOTP or Dynamic Host Configuration Protocol (DHCP) server, then the default domain name might be set by the BOOTP or DHCP server (if the servers were configured with this information).
Step 4	**ip name-server** *server-address1* [*server-address2 ... server-address6*]	Specifies the address of one or more name servers to use for name and address resolution.

	Command or Action	Purpose
	Example: `Switch(config)# ip name-server 192.168.1.100 192.168.1.200 192.168.1.300`	You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The switch sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 5	**ip domain-lookup** [**nsap** | **source-interface** *interface*] **Example:** `Switch(config)# ip domain-lookup`	(Optional) Enables DNS-based hostname-to-address translation on your switch. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS).
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring a Message-of-the-Day Login Banner

You can create a single or multiline message banner that appears on the screen when someone logs in to the switch

Follow these steps to configure a MOTD login banner:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Switch> enable`	
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

Step 3	**banner motd** *c message c*
	Example:
	`Switch(config)# banner motd #`
	`This is a secure site. Only`
	`authorized users are allowed.`
	`For access, contact technical`
	`support.`
	`#`
		Specifies the message of the day.
		c—Enters the delimiting character of your choice, for example, a pound sign (#), and press the **Return** key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.
		message—Enters a banner message up to 255 characters. You cannot use the delimiting character in the message.

Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring a Login Banner

You can configure a login banner to be displayed on all connected terminals. This banner appears after the MOTD banner and before the login prompt.

Follow these steps to configure a login banner:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

Step 3	**banner login** *c message c*
	Example:
	`Switch(config)# banner login $`
	`Access for authorized users only.`
	`Please enter your username and password.`
	`$`
		Specifies the login message.
		c— Enters the delimiting character of your choice, for example, a pound sign (#), and press the **Return** key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.
		message—Enters a login message up to 255 characters. You cannot use the delimiting character in the message.

Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Managing the MAC Address Table

Changing the Address Aging Time

Follow these steps to configure the dynamic address table aging time:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**mac address-table aging-time** [*0* | *10-1000000*] [**routed-mac** | **vlan** *vlan-id*] **Example:** `Switch(config)# mac address-table aging-time 500 vlan 2`	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. The range is 10 to 1000000 seconds. The default is 300. You can also enter 0, which disables aging. Static address entries are never aged or removed from the table. *vlan-id*—Valid IDs are 1 to 4094.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring MAC Address Change Notification Traps

Follow these steps to configure the switch to send MAC address change notification traps to an NMS host:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**snmp-server host** *host-addr community-string notification-type* { **informs** | **traps** } {**version** {**1** | **2c** | **3**}} {**vrf** *vrf instance name*} **Example:** `Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification`	Specifies the recipient of the trap message. • *host-addr*—Specifies the name or address of the NMS. • **traps** (the default)—Sends SNMP traps to the host. • **informs**—Sends SNMP informs to the host. • **version**—Specifies the SNMP version to support. Version 1, the default, is not available with informs. • *community-string*—Specifies the string to send with the notification operation. Though you can set this string by using the **snmp-server host** command, we recommend that you define this string by using the **snmp-server community** command before using the **snmp-server host** command. • *notification-type*—Uses the **mac-notification** keyword. • **vrf** *vrf instance name*—Specifies the VPN routing/forwarding instance for this host.
Step 4	**snmp-server enable traps mac-notification change** **Example:**	Enables the switch to send MAC address change notification traps to the NMS.

	Command or Action	Purpose
	`Switch(config)# snmp-server enable traps mac-notification change`	
Step 5	**mac address-table notification change** **Example:** `Switch(config)# mac address-table notification change`	Enables the MAC address change notification feature.

Step 6	**mac address-table notification change** [**interval** *value*] [**history-size** *value*]
	Example:
	`Switch(config)# mac address-table notification change interval 123`
	`Switch(config)#mac address-table notification change history-size 100`
		Enters the trap interval time and the history table size.
		• (Optional) **interval** *value*—Specifies the notification trap interval in seconds between each set of traps that are generated to the NMS. The range is 0 to 2147483647 seconds; the default is 1 second.
		• (Optional) **history-size** *value*—Specifies the maximum number of entries in the MAC notification history table. The range is 0 to 500; the default is 1.

Step 7	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/2`	Enters interface configuration mode, and specifies the Layer 2 interface on which to enable the SNMP MAC address notification trap.
Step 8	**snmp trap mac-notification change** {**added** | **removed**} **Example:** `Switch(config-if)# snmp trap mac-notification change added`	Enables the MAC address change notification trap on the interface. • Enables the trap when a MAC address is **added** on this interface. • Enables the trap when a MAC address is **removed** from this interface.
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 10	**show running-config** **Example:**	Verifies your entries.

	Command or Action	Purpose
	`Switch# show running-config`	
Step 11	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring MAC Address Move Notification Traps

When you configure MAC-move notification, an SNMP notification is generated and sent to the network management system whenever a MAC address moves from one port to another within the same VLAN.

Follow these steps to configure the switch to send MAC address-move notification traps to an NMS host:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type* **Example:** `Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification`	Specifies the recipient of the trap message. • *host-addr*—Specifies the name or address of the NMS. • **traps** (the default)—Sends SNMP traps to the host. • **informs**—Sends SNMP informs to the host. • **version**—Specifies the SNMP version to support. Version 1, the default, is not available with informs. • *community-string*—Specifies the string to send with the notification operation. Though you can set this string by using the **snmp-server host** command, we

	Command or Action	Purpose
		recommend that you define this string by using the **snmp-server community** command before using the **snmp-server host** command. • *notification-type*—Uses the **mac-notification** keyword.
Step 4	**snmp-server enable traps mac-notification move** **Example:** `Switch(config)# snmp-server enable traps mac-notification move`	Enables the switch to send MAC address move notification traps to the NMS.
Step 5	**mac address-table notification mac-move** **Example:** `Switch(config)# mac address-table notification mac-move`	Enables the MAC address move notification feature.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

To disable MAC address-move notification traps, use the **no snmp-server enable traps mac-notification move** global configuration command. To disable the MAC address-move notification feature, use the **no mac address-table notification mac-move** global configuration command.

You can verify your settings by entering the **show mac address-table notification mac-move** privileged EXEC commands.

Configuring MAC Threshold Notification Traps

When you configure MAC threshold notification, an SNMP notification is generated and sent to the network management system when a MAC address table threshold limit is reached or exceeded.

Follow these steps to configure the switch to send MAC address table threshold notification traps to an NMS host:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type* **Example:** `Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification`	Specifies the recipient of the trap message. • *host-addr*—Specifies the name or address of the NMS. • **traps** (the default)—Sends SNMP traps to the host. • **informs**—Sends SNMP informs to the host. • **version**—Specifies the SNMP version to support. Version 1, the default, is not available with informs. • *community-string*—Specifies the string to send with the notification operation. You can set this string by using the **snmp-server host** command, but we recommend that you define this string by using the **snmp-server community** command before using the **snmp-server host** command. • *notification-type*—Uses the **mac-notification** keyword.

	Command or Action	Purpose
Step 4	**snmp-server enable traps mac-notification threshold** **Example:** `Switch(config)# snmp-server enable traps mac-notification threshold`	Enables MAC threshold notification traps to the NMS.
Step 5	**mac address-table notification threshold** **Example:** `Switch(config)# mac address-table notification threshold`	Enables the MAC address threshold notification feature.

Step 6	**mac address-table notification threshold** [**limit** *percentage*] | [**interval** *time*]
	Example:
	`Switch(config)# mac address-table notification threshold interval 123`
	`Switch(config)# mac address-table notification threshold limit 78`
		Enters the threshold value for the MAC address threshold usage monitoring.
		• (Optional) **limit** *percentage*—Specifies the percentage of the MAC address table use; valid values are from 1 to 100 percent. The default is 50 percent.
		• (Optional) **interval** *time*—Specifies the time between notifications; valid values are greater than or equal to 120 seconds. The default is 120 seconds.

Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 8	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 9	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Adding and Removing Static Address Entries

Follow these steps to add a static address:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* **Example:** `Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet 1/0/1`	Adds a static address to the MAC address table. • *mac-addr*—Specifies the destination MAC unicast address to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface. • *vlan-id*—Specifies the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094. • *interface-id*—Specifies the interface to which the received packet is forwarded. Valid interfaces include physical ports or port channels. For static multicast addresses, you can enter multiple interface IDs. For static unicast addresses, you can enter only one interface at a time, but you can enter the command multiple times with the same MAC address and VLAN ID.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.

	Command or Action	Purpose
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Unicast MAC Address Filtering

Follow these steps to configure the Switch to drop a source or destination unicast static address:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** **Example:** `Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop`	Enables unicast MAC address filtering and configure the switch to drop a packet with the specified source or destination unicast static address. • *mac-addr*—Specifies a source or destination unicast MAC address (48-bit). Packets with this MAC address are dropped. • *vlan-id*—Specifies the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Monitoring and Maintaining Administration of the Switch

Command	Purpose
clear mac address-table dynamic	Removes all dynamic entries.
clear mac address-table dynamic address *mac-address*	Removes a specific MAC address.
clear mac address-table dynamic interface *interface-id*	Removes all addresses on the specified physical port or port channel.
clear mac address-table dynamic vlan *vlan-id*	Removes all addresses on a specified VLAN.
show clock [*detail*]	Displays the time and date configuration.
show ip igmp snooping groups	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table address *mac-address*	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays only dynamic MAC address table entries.
show mac address-table interface *interface-name*	Displays the MAC address table information for the specified interface.
show mac address-table move update	Displays the MAC address table move update information.
show mac address-table multicast	Displays a list of multicast MAC addresses.

Command	Purpose
show mac address-table notification {change | mac-move | threshold}	Displays the MAC notification parameters and history table.
show mac address-table secure	Displays the secure MAC addresses.
show mac address-table static	Displays only static MAC address table entries.
show mac address-table vlan *vlan-id*	Displays the MAC address table information for the specified VLAN.

Configuration Examples for Switch Administration

Example: Setting the System Clock

This example shows how to manually set the system clock:

```
Switch# clock set 13:32:00 23 July 2013
```

Examples: Configuring Summer Time

This example (for daylight savings time) shows how to specify that summer time starts on March 10 at 02:00 and ends on November 3 at 02:00:

```
Switch(config)# clock summer-time PDT recurring PST date
10 March 2013 2:00 3 November 2013 2:00
```

This example shows how to set summer time start and end dates:

```
Switch(config)#clock summer-time PST date
20 March 2013 2:00 20 November 2013 2:00
```

Example: Configuring a MOTD Banner

This example shows how to configure a MOTD banner by using the pound sign (#) symbol as the beginning and ending delimiter:

```
Switch(config)# banner motd #

This is a secure site. Only authorized users are allowed.
For access, contact technical support.

#

Switch(config)#
```

This example shows the banner that appears from the previous configuration:

```
Unix> telnet 192.0.2.15

Trying 192.0.2.15...

Connected to 192.0.2.15.

Escape character is '^]'.

This is a secure site. Only authorized users are allowed.

For access, contact technical support.

User Access Verification

Password:
```

Example: Configuring a Login Banner

This example shows how to configure a login banner by using the dollar sign ($) symbol as the beginning and ending delimiter:

```
Switch(config)# banner login $

Access for authorized users only. Please enter your username and password.

$

Switch(config)#
```

Example: Configuring MAC Address Change Notification Traps

This example shows how to specify 172.20.10.10 as the NMS, enable MAC address notification traps to the NMS, enable the MAC address-change notification feature, set the interval time to 123 seconds, set the history-size to 100 entries, and enable traps whenever a MAC address is added on the specified port:

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification change
Switch(config)# mac address-table notification change
Switch(config)# mac address-table notification change interval 123
Switch(config)# mac address-table notification change history-size 100
Switch(config)# interface gigabitethernet1/2/1
Switch(config-if)# snmp trap mac-notification change added
```

Example: Configuring MAC Threshold Notification Traps

This example shows how to specify 172.20.10.10 as the NMS, enable the MAC address threshold notification feature, set the interval time to 123 seconds, and set the limit to 78 per cent:

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
```

```
Switch(config)# snmp-server enable traps mac-notification threshold
Switch(config)# mac address-table notification threshold
Switch(config)# mac address-table notification threshold interval 123
Switch(config)# mac address-table notification threshold limit 78
```

Example: Adding the Static Address to the MAC Address Table

This example shows how to add the static address c2f3.220a.12f4 to the MAC address table. When a packet is received in VLAN 4 with this MAC address as its destination address, the packet is forwarded to the specified port:

Note You cannot associate the same static MAC address to multiple interfaces. If the command is executed again with a different interface, the static MAC address is overwritten on the new interface.

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet1/1/1
```

Example: Configuring Unicast MAC Address Filtering

This example shows how to enable unicast MAC address filtering and how to configure drop packets that have a source or destination address of c2f3.220a.12f4. When a packet is received in VLAN 4 with this MAC address as its source or destination, the packet is dropped:

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

Additional References for Switch Administration

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference (Catalyst 3850 Switches)System Management Command Reference (Cisco WLC 5700 Series)*
Network management configuration	*Network Management Configuration Guide (Catalyst 3850 Switches) Network Management Configuration Guide (Cisco WLC 5700 Series)*

Related Topic	Document Title
Layer 2 configuration	*Layer 2/3 Configuration Guide (Catalyst 3850 Switches)Layer 2 Configuration Guide (Cisco WLC 5700 Series)*
VLAN configuration	*VLAN Configuration Guide (Catalyst 3850 Switches) VLAN Configuration Guide (Cisco WLC 5700 Series)*
Platform-independent command references	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*
Platform-independent configuration information	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3850 Switches)* *IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

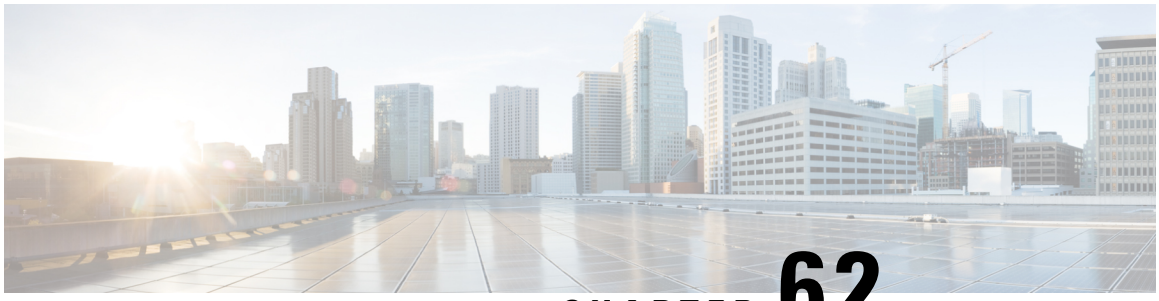
MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for Switch Administration

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 62

Performing Switch Setup Configuration

Information About Performing Switch Setup Configuration

Review the sections in this module before performing your initial switch configuration tasks that include IP address assignments and DHCP autoconfiguration.

Switch Boot Process

To start your switch, you need to follow the procedures in the hardware installation guide for installing and powering on the switch and setting up the initial switch configuration (IP address, subnet mask, default gateway, secret and Telnet passwords, and so forth).

The normal boot process involves the operation of the boot loader software and includes these activities:

- Performs low-level CPU initialization. It initializes the CPU registers, which control where physical memory is mapped, its quantity, its speed, and so forth.
- Performs power-on self-test (POST) for the CPU subsystem and tests the system DRAM.
- Initializes the file systems on the system board.
- Loads a default operating system software image into memory and boots up the switch.

The boot loader provides access to the file systems before the operating system is loaded. Normally, the boot loader is used only to load, decompress, and start the operating system. After the boot loader gives the operating system control of the CPU, the boot loader is not active until the next system reset or power-on.

The boot loader also provides trap-door access into the system if the operating system has problems serious enough that it cannot be used. The trap-door mechanism provides enough access to the system so that if it is necessary, you can reinstall the operating system software image by using the Xmodem Protocol, recover from a lost or forgotten password, and finally restart the operating system.

Before you can assign switch information, make sure you have connected a PC or terminal to the console port or a PC to the Ethernet management port, and make sure you have configured the PC or terminal-emulation software baud rate and character format to match these of the switch console port:

- Baud rate default is 9600.
- Data bits default is 8.

Note If the data bits option is set to 8, set the parity option to none.

- Stop bits default is 2 (minor).
- Parity settings default is none.

Software Installer Features

The following software installer features are supported on your switch:

- Software bundle installation on a standalone switch.
- Software rollback to a previously installed package set.
- Emergency installation in the event that no valid installed packages reside on the boot flash.

Software Boot Modes

Your switch supports two modes to boot the software packages:

- Installed mode
- Bundle mode

Related Topics

Examples: Displaying Software Bootup in Install Mode, on page 1231
Example: Emergency Installation, on page 1233

Installed Boot Mode

You can boot your switch in installed mode by booting the software package provisioning file that resides in flash:

```
Switch: boot flash:packages.conf
```

The provisioning file contains a list of software packages to boot, mount, and run. The ISO file system in each installed package is mounted to the root file system directly from flash.

Note The packages and provisioning file used to boot in installed mode must reside in flash. Booting in installed mode from usbflash0: or tftp: is not supported.

Related Topics

Examples: Displaying Software Bootup in Install Mode, on page 1231
Example: Emergency Installation, on page 1233

Bundle Boot Mode

You can boot your switch in bundle boot mode by booting the bundle (.bin) file:

The provisioning file contained in a bundle is used to decide which packages to boot, mount, and run. Packages are extracted from the bundle and copied to RAM. The ISO file system in each package is mounted to the root file system.

Unlike install boot mode, additional memory that is equivalent to the size of the bundle is used when booting in bundle mode.

Note Auto install and smart install functionality is not supported in bundle boot mode.

Related Topics

Examples: Displaying Software Bootup in Install Mode, on page 1231
Example: Emergency Installation, on page 1233

Switches Information Assignment

You can assign IP information through the switch setup program, through a DHCP server, or manually.

Use the switch setup program if you want to be prompted for specific IP information. With this program, you can also configure a hostname and an enable secret password.

It gives you the option of assigning a Telnet password (to provide security during remote management) and configuring your switch as a command or member switch of a cluster or as a standalone switch.

Use a DHCP server for centralized control and automatic assignment of IP information after the server is configured.

Note If you are using DHCP, do not respond to any of the questions in the setup program until the switch receives the dynamically assigned IP address and reads the configuration file.

If you are an experienced user familiar with the switch configuration steps, manually configure the switch. Otherwise, use the setup program described in the *Boot Process* section.

DHCP-Based Autoconfiguration Overview

DHCP provides configuration information to Internet hosts and internetworking devices. This protocol consists of two components: one for delivering configuration parameters from a DHCP server to a device and an operation for allocating network addresses to devices. DHCP is built on a client-server model, in which designated DHCP servers allocate network addresses and deliver configuration parameters to dynamically configured devices. The switch can act as both a DHCP client and a DHCP server.

During DHCP-based autoconfiguration, your switch (DHCP client) is automatically configured at startup with IP address information and a configuration file.

With DHCP-based autoconfiguration, no DHCP client-side configuration is needed on your switch. However, you need to configure the DHCP server for various lease options associated with IP addresses.

If you want to use DHCP to relay the configuration file location on the network, you might also need to configure a Trivial File Transfer Protocol (TFTP) server and a Domain Name System (DNS) server.

The DHCP server for your switch can be on the same LAN or on a different LAN than the switch. If the DHCP server is running on a different LAN, you should configure a DHCP relay device between your switch and the DHCP server. A relay device forwards broadcast traffic between two directly connected LANs. A router does not forward broadcast packets, but it forwards packets based on the destination IP address in the received packet.

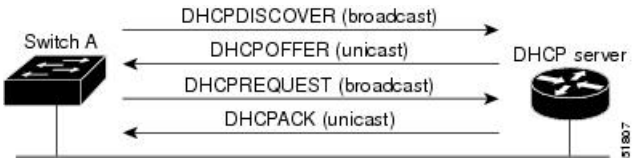
DHCP-based autoconfiguration replaces the BOOTP client functionality on your switch.

DHCP Client Request Process

When you boot up your switch, the DHCP client is invoked and requests configuration information from a DHCP server when the configuration file is not present on the switch. If the configuration file is present and the configuration includes the **ip address dhcp** interface configuration command on specific routed interfaces, the DHCP client is invoked and requests the IP address information for those interfaces.

This is the sequence of messages that are exchanged between the DHCP client and the DHCP server.

Figure 70: DHCP Client and Server Message Exchange



The client, Switch A, broadcasts a DHCPDISCOVER message to locate a DHCP server. The DHCP server offers configuration parameters (such as an IP address, subnet mask, gateway IP address, DNS IP address, a lease for the IP address, and so forth) to the client in a DHCPOFFER unicast message.

In a DHCPREQUEST broadcast message, the client returns a formal request for the offered configuration information to the DHCP server. The formal request is broadcast so that all other DHCP servers that received the DHCPDISCOVER broadcast message from the client can reclaim the IP addresses that they offered to the client.

The DHCP server confirms that the IP address has been allocated to the client by returning a DHCPACK unicast message to the client. With this message, the client and server are bound, and the client uses configuration information received from the server. The amount of information the switch receives depends on how you configure the DHCP server.

If the configuration parameters sent to the client in the DHCPOFFER unicast message are invalid (a configuration error exists), the client returns a DHCPDECLINE broadcast message to the DHCP server.

The DHCP server sends the client a DHCPNAK denial broadcast message, which means that the offered configuration parameters have not been assigned, that an error has occurred during the negotiation of the parameters, or that the client has been slow in responding to the DHCPOFFER message (the DHCP server assigned the parameters to another client).

A DHCP client might receive offers from multiple DHCP or BOOTP servers and can accept any of the offers; however, the client usually accepts the first offer it receives. The offer from the DHCP server is not a guarantee

that the IP address is allocated to the client; however, the server usually reserves the address until the client has had a chance to formally request the address. If the switch accepts replies from a BOOTP server and configures itself, the switch broadcasts, instead of unicasts, TFTP requests to obtain the switch configuration file.

The DHCP hostname option allows a group of switches to obtain hostnames and a standard configuration from the central management DHCP server. A client (switch) includes in its DCHPDISCOVER message an option 12 field used to request a hostname and other configuration parameters from the DHCP server. The configuration files on all clients are identical except for their DHCP-obtained hostnames.

If a client has a default hostname (the **hostname** *name* global configuration command is not configured or the **no hostname** global configuration command is entered to remove the hostname), the DHCP hostname option is not included in the packet when you enter the **ip address dhcp** interface configuration command. In this case, if the client receives the DCHP hostname option from the DHCP interaction while acquiring an IP address for an interface, the client accepts the DHCP hostname option and sets the flag to show that the system now has a hostname configured.

DHCP Server Configuration Guidelines

Follow these guidelines if you are configuring a device as a DHCP server:

- You should configure the DHCP server with reserved leases that are bound to each switch by the switch hardware address.
- If you want the switch to receive IP address information, you must configure the DHCP server with these lease options:
  - IP address of the client (required)
  - Subnet mask of the client (required)
  - DNS server IP address (optional)
  - Router IP address (default gateway address to be used by the switch) (required)
- If you want the switch to receive the configuration file from a TFTP server, you must configure the DHCP server with these lease options:
  - TFTP server name (required)
  - Boot filename (the name of the configuration file that the client needs) (recommended)
  - Hostname (optional)
- Depending on the settings of the DHCP server, the switch can receive IP address information, the configuration file, or both.
- If you do not configure the DHCP server with the lease options described previously, it replies to client requests with only those parameters that are configured. If the IP address and the subnet mask are not in the reply, the switch is not configured. If the router IP address or the TFTP server name are not found, the switch might send broadcast, instead of unicast, TFTP requests. Unavailability of other lease options does not affect autoconfiguration.
- The switch can act as a DHCP server. By default, the Cisco IOS DHCP server and relay agent features are enabled on your switch but are not configured. (These features are not operational.)

Purpose of the TFTP Server

Based on the DHCP server configuration, the switch attempts to download one or more configuration files from the TFTP server. If you configured the DHCP server to respond to the switch with all the options required for IP connectivity to the TFTP server, and if you configured the DHCP server with a TFTP server name, address, and configuration filename, the switch attempts to download the specified configuration file from the specified TFTP server.

If you did not specify the configuration filename, the TFTP server, or if the configuration file could not be downloaded, the switch attempts to download a configuration file by using various combinations of filenames and TFTP server addresses. The files include the specified configuration filename (if any) and these files: network-config, cisconet.cfg, *hostname*.config, or *hostname*.cfg, where *hostname* is the switch's current hostname. The TFTP server addresses used include the specified TFTP server address (if any) and the broadcast address (255.255.255.255).

For the switch to successfully download a configuration file, the TFTP server must contain one or more configuration files in its base directory. The files can include these files:

- The configuration file named in the DHCP reply (the actual switch configuration file).
- The network-confg or the cisconet.cfg file (known as the default configuration files).
- The router-confg or the ciscortr.cfg file (These files contain commands common to all switches. Normally, if the DHCP and TFTP servers are properly configured, these files are not accessed.)

If you specify the TFTP server name in the DHCP server-lease database, you must also configure the TFTP server name-to-IP-address mapping in the DNS-server database.

If the TFTP server to be used is on a different LAN from the switch, or if it is to be accessed by the switch through the broadcast address (which occurs if the DHCP server response does not contain all the required information described previously), a relay must be configured to forward the TFTP packets to the TFTP server. The preferred solution is to configure the DHCP server with all the required information.

Purpose of the DNS Server

The DHCP server uses the DNS server to resolve the TFTP server name to an IP address. You must configure the TFTP server name-to-IP address map on the DNS server. The TFTP server contains the configuration files for the switch.

You can configure the IP addresses of the DNS servers in the lease database of the DHCP server from where the DHCP replies will retrieve them. You can enter up to two DNS server IP addresses in the lease database.

The DNS server can be on the same LAN or on a different LAN from the switch. If it is on a different LAN, the switch must be able to access it through a router.

How to Obtain Configuration Files

Depending on the availability of the IP address and the configuration filename in the DHCP reserved lease, the switch obtains its configuration information in these ways:

- The IP address and the configuration filename is reserved for the switch and provided in the DHCP reply (one-file read method).

  The switch receives its IP address, subnet mask, TFTP server address, and the configuration filename from the DHCP server. The switch sends a unicast message to the TFTP server to retrieve the named configuration file from the base directory of the server and upon receipt, it completes its boot up process.

- The IP address and the configuration filename is reserved for the switch, but the TFTP server address is not provided in the DHCP reply (one-file read method).

  The switch receives its IP address, subnet mask, and the configuration filename from the DHCP server. The switch sends a broadcast message to a TFTP server to retrieve the named configuration file from the base directory of the server, and upon receipt, it completes its boot-up process.

- Only the IP address is reserved for the switch and provided in the DHCP reply. The configuration filename is not provided (two-file read method).

  The switch receives its IP address, subnet mask, and the TFTP server address from the DHCP server. The switch sends a unicast message to the TFTP server to retrieve the network-confg or cisconet.cfg default configuration file. (If the network-confg file cannot be read, the switch reads the cisconet.cfg file.)

  The default configuration file contains the hostnames-to-IP-address mapping for the switch. The switch fills its host table with the information in the file and obtains its hostname. If the hostname is not found in the file, the switch uses the hostname in the DHCP reply. If the hostname is not specified in the DHCP reply, the switch uses the default *Switch* as its hostname.

  After obtaining its hostname from the default configuration file or the DHCP reply, the switch reads the configuration file that has the same name as its hostname (*hostname*-confg or *hostname*.cfg, depending on whether network-confg or cisconet.cfg was read earlier) from the TFTP server. If the cisconet.cfg file is read, the filename of the host is truncated to eight characters.

  If the switch cannot read the network-confg, cisconet.cfg, or the hostname file, it reads the router-confg file. If the switch cannot read the router-confg file, it reads the ciscortr.cfg file.

Note The switch broadcasts TFTP server requests if the TFTP server is not obtained from the DHCP replies, if all attempts to read the configuration file through unicast transmissions fail, or if the TFTP server name cannot be resolved to an IP address.

How to Control Environment Variables

With a normally operating switch, you enter the boot loader mode only through the console connection configured for 9600 bps. Unplug the switch power cord, and press the **Mode** button while reconnecting the power cord. You can release the **Mode** button after all the amber system LEDs turn on and remain solid. The boot loader switch prompt then appears.

The switch boot loader software provides support for nonvolatile environment variables, which can be used to control how the boot loader, or any other software running on the system, operates. Boot loader environment variables are similar to environment variables that can be set on UNIX or DOS systems.

Environment variables that have values are stored in flash memory outside of the flash file system.

Each line in these files contains an environment variable name and an equal sign followed by the value of the variable. A variable has no value if it is not present; it has a value if it is listed even if the value is a null string. A variable that is set to a null string (for example, “ ”) is a variable with a value. Many environment variables are predefined and have default values.

You can change the settings of the environment variables by accessing the boot loader or by using Cisco IOS commands. Under normal circumstances, it is not necessary to alter the setting of the environment variables.

Scheduled Reload of the Software Image

You can schedule a reload of the software image to occur on the switch at a later time (for example, late at night or during the weekend when the switch is used less), or you can synchronize a reload network-wide (for example, to perform a software upgrade on all switches in the network).

You have these reload options:

- Reload of the software to take affect in the specified minutes or hours and minutes. The reload must take place within approximately 24 hours. You can specify the reason for the reload in a string up to 255 characters in length.
- Reload of the software to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time) or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight.

The **reload** command halts the system. If the system is not set to manually boot up, it reboots itself.

If your switch is configured for manual booting, do not reload it from a virtual terminal. This restriction prevents the switch from entering the boot loader mode and then taking it from the remote user's control.

If you modify your configuration file, the switch prompts you to save the configuration before reloading. During the save operation, the system requests whether you want to proceed with the save if the CONFIG_FILE environment variable points to a startup configuration file that no longer exists. If you proceed in this situation, the system enters setup mode upon reload.

To cancel a previously scheduled reload, use the **reload cancel** privileged EXEC command.

How to Perform Switch Setup Configuration

Using DHCP to download a new image and a new configuration to a switch requires that you configure at least two switches. One switch acts as a DHCP and TFTP server and the second switch (client) is configured to download either a new configuration file or a new configuration file and a new image file.

Configuring DHCP Autoconfiguration (Only Configuration File)

This task describes how to configure DHCP autoconfiguration of the TFTP and DHCP settings on an existing switch in the network so that it can support the autoconfiguration of a new switch.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ip dhcp pool** *poolname* **Example:** `Switch(config)# ip dhcp pool pool`	Creates a name for the DHCP server address pool, and enters DHCP pool configuration mode.
Step 3	**boot** *filename* **Example:** `Switch(dhcp-config)# boot config-boot.text`	Specifies the name of the configuration file that is used as a boot image.
Step 4	**network** *network-number mask prefix-length* **Example:** `Switch(dhcp-config)# network 10.10.10.0 255.255.255.0`	Specifies the subnet network number and mask of the DHCP address pool. **Note** The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).
Step 5	**default-router** *address* **Example:** `Switch(dhcp-config)# default-router 10.10.10.1`	Specifies the IP address of the default router for a DHCP client.
Step 6	**option 150** *address* **Example:** `Switch(dhcp-config)# option 150 10.10.10.1`	Specifies the IP address of the TFTP server.
Step 7	**exit** **Example:** `Switch(dhcp-config)# exit`	Returns to global configuration mode.
Step 8	**tftp-server flash**:*filename.text* **Example:** `Switch(config)# tftp-server flash:config-boot.text`	Specifies the configuration file on the TFTP server.

	Command or Action	Purpose
Step 9	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/4`	Specifies the address of the client that will receive the configuration file.
Step 10	**no switchport** **Example:** `Switch(config-if)# no switchport`	Puts the interface into Layer 3 mode.
Step 11	**ip address** *address mask* **Example:** `Switch(config-if)# ip address 10.10.10.1 255.255.255.0`	Specifies the IP address and mask for the interface.
Step 12	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Manually Assigning IP Information to Multiple SVIs

This task describes how to manually assign IP information to multiple switched virtual interfaces (SVIs):

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**interface vlan** *vlan-id* **Example:** `Switch(config)# interface vlan 99`	Enters interface configuration mode, and enters the VLAN to which the IP information is assigned. The range is 1 to 4094.
Step 3	**ip address** *ip-address subnet-mask* **Example:**	Enters the IP address and subnet mask.

	Command or Action	Purpose
	`Switch(config-vlan)# ip address 10.10.10.2 255.255.255.0`	
Step 4	**exit** **Example:** `Switch(config-vlan)# exit`	Returns to global configuration mode.
Step 5	**ip default-gateway** *ip-address* **Example:** `Switch(config)# ip default-gateway 10.10.10.1`	Enters the IP address of the next-hop router interface that is directly connected to the switch where a default gateway is being configured. The default gateway receives IP packets with unresolved destination IP addresses from the switch. Once the default gateway is configured, the switch has connectivity to the remote networks with which a host needs to communicate. **Note** When your switch is configured to route with IP, it does not need to have a default gateway set. **Note** The switch capwap relays on default-gateway configuration to support routed access point join the switch.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	**show interfaces vlan** *vlan-id* **Example:** `Switch# show interfaces vlan 99`	Verifies the configured IP address.
Step 8	**show ip redirects** **Example:** `Switch# show ip redirects`	Verifies the configured default gateway.

Modifying the Switch Startup Configuration

Specifying the Filename to Read and Write the System Configuration

By default, the Cisco IOS software uses the config.text file to read and write a nonvolatile copy of the system configuration. However, you can specify a different filename, which will be loaded during the next boot cycle.

Before you begin

Use a standalone switch for this task.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**boot flash**:*//file-url* **Example:** `Switch(config)# boot flash:config.text`	Specifies the configuration file to load during the next boot cycle. *file-url*—The path (directory) and the configuration filename. Filenames and directory names are case-sensitive.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 4	**show boot** **Example:** `Switch# show boot`	Verifies your entries. The **boot** global configuration command changes the setting of the CONFIG_FILE environment variable.
Step 5	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Booting the Switch in Installed Mode

Procedure

	Command or Action	Purpose
Step 1	**cp** *source_file_path destination_file_path* **Example:** `Switch#` **`copy`** **`tftp://10.0.0.6/cat3k_caa-universalk9.SSA.03.12.02.EXP.150-12.02.EXP.150-12.02.EXP.bin`**`flash:`**	(Optional) Copies the bin file (`image.bin`) from the FTP or TFTP server to USB flash.

Step 2	**Example:**
	Expanding the bin file from the TFTP server:
	`Switch# request platform software package expand switch all file tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin to flash:`
	`Preparing expand operation ...`
	`[1]: Downloading file tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin to active switch 1`
	`[1]: Finished downloading file tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin to active switch 1`
	`[1]: Copying software from active switch 1 to switch 2`
	`[1]: Finished copying software to switch 2`
	`[1 2]: Expanding bundle cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin`
	`[1 2]: Copying package files`
	`[1 2]: Package files copied`
	`[1 2]: Finished expanding bundle cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin`
	
	`18 -rw- 74387812 Dec 7 2012 05:55:43 +00:00 cat3k_caa-base.SSA.03.09.37.EXP.pkg`
	`19 -rw- 2738868 Dec 7 2012 05:55:44 +00:00 cat3k_caa-drivers.SSA.03.09.37.EXP.pkg`
	`20 -rw- 32465772 Dec 7 2012 05:55:44 +00:00 cat3k_caa-infra.SSA.03.09.37.EXP.pkg`
	`21 -rw- 30389036 Dec 7 2012 05:55:44 +00:00 cat3k_caa-iosd-universalk9.SSA.150-9.37.EXP.pkg`
	
	`22 -rw- 18342624 Dec 7 2012 05:55:44 +00:00 cat3k_caa-platform.SSA.03.09.37.EXP.pkg`
	`23 -rw- 63374028 Dec 7 2012 05:55:44 +00:00 cat3k_caa-wcm.SSA.10.0.10.14.pkg`
	`17 -rw- 1239 Dec 7 2012 05:56:29 +00:00 packages.conf`
		Expands the bin file stored in flash, FTP, TFTP, HTTP, or HTTPS server on the booted switch.
		Note Ensure that the `packages.conf` file is available in the expanded list.

	Command or Action	Purpose
Step 3	**reload** **Example:** `Switch# reload`	Reloads the switch. **Note** You can boot the switch manually or automatically using the `packages.conf` file. If you are booting manually, you can proceed to Step 4. Otherwise, the switch boots up automatically.
Step 4	**boot flash:packages.conf** **Example:** `Switch: boot flash:packages.conf`	Boots the switch with the `packages.conf` file.

Step 5	**show version**
	Example:
	`switch# show version`
	
	`Switch Ports Model SW Version SW Image Mode`
	
	`------ ----- ----- ---------- ---------- ----`
	`1 6 WS-C3850-6DS-S 03.09.26.EXP ct3850-ipservicesk9 INSTALL`
		Verifies that the switch is in the **INSTALL** mode.

Booting the Switch in Bundle Mode

There are several methods by which you can boot the switch—either by copying the bin file from the TFTP server and then boot the switch, or by booting the switch straight from flash or USB flash using the commands **boot flash:<image.bin>** or **boot usbflash0:<image.bin>** .

The following procedure explains how to boot the switch from the TFTP server in the bundle mode.

Procedure

	Command or Action	Purpose
Step 1	**switch:BOOT=<source path of .bin file>** **Example:** `switch:BOOT=tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin`	Sets the boot parameters.
Step 2	**boot** **Example:** `switch: boot`	Boots the switch.
Step 3	**show version** **Example:**	Verifies that the switch is in the **BUNDLE** mode.

	Command or Action	Purpose

	`switch# show version`
	
	`Switch Ports Model SW Version SW Image Mode`
	
	`------ ----- ----- ---------- ---------- ----`
	`1 6 WS-C3850-6DS-S 03.09.40.EXP ct3850-ipservicesk9 BUNDLE`	

Configuring a Scheduled Software Image Reload

This task describes how to configure your switch to reload the software image at a later time.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**copy running-config startup-config** **Example:** `copy running-config startup-config`	Saves your switch configuration information to the startup configuration before you use the **reload** command.

Step 3	**reload in** [*hh*:]*mm* [*text*]
	Example:
	`Switch(config)# reload in 12`
	
	`System configuration has been modified. Save? [yes/no]: y`
		Schedules a reload of the software to take affect in the specified minutes or hours and minutes. The reload must take place within approximately 24 days. You can specify the reason for the reload in a string up to 255 characters in length.

Step 4	**reload slot** [*stack-member-number*]
	Example:
	`Switch(config)# reload slot 6`
	
	`Proceed with reload? [confirm] y`
		Schedules a reload of the software in a switch stack.

Step 5	**reload at** *hh*: *mm* [*month day* | *day month*] [*text*] **Example:**	Specifies the time in hours and minutes for the reload to occur.

	Command or Action	Purpose
	`Switch(config)# reload at 14:00`	**Note** Use the **at** keyword only if the switch system clock has been set (through Network Time Protocol (NTP), the hardware calendar, or manually). The time is relative to the configured time zone on the switch. To schedule reloads across several switches to occur simultaneously, the time on each switch must be synchronized with NTP.
Step 6	**reload cancel** **Example:** `Switch(config)# reload cancel`	Cancels a previously scheduled reload.
Step 7	**show reload** **Example:** `show reload`	Displays information about a previously scheduled reload or identifies if a reload has been scheduled on the switch.

Monitoring Switch Setup Configuration

Example: Verifying the Switch Running Configuration

```
Switch# show running-config
Building configuration...

Current configuration: 1363 bytes
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Stack1
!
enable secret 5 $1$ej9.$DMUvAUnZOAmvmgqBEzIxE0
!
.
<output truncated>
.
interface gigabitethernet6/0/2
mvr type source

<output truncated>

...!
interface VLAN1
 ip address 172.20.137.50 255.255.255.0
```

```
 no ip directed-broadcast
!
ip default-gateway 172.20.137.1 !
!
snmp-server community private RW
snmp-server community public RO
snmp-server community private@es0 RW
snmp-server community public@es0 RO
snmp-server chassis-id 0x12
!
end
```

Examples: Displaying Software Bootup in Install Mode

This example displays software bootup in install mode:

```
switch: boot flash:packages.conf

Getting rest of image
Reading full image into memory....done
Reading full base package into memory...: done = 74596432
Nova Bundle Image
--------------------------------------
Kernel Address : 0x6042f354
Kernel Size : 0x318412/3245074
Initramfs Address : 0x60747768
Initramfs Size : 0xdc08e8/14420200
Compression Format: .mzip

Bootable image at @ ram:0x6042f354
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000,
0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@boot_system:
 377
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)

All packages are Digitally Signed
Starting System Services
Nov 7 09:57:05 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_START: Switch 2 is
starting stack discovery
##########################################################################################################################
Nov 7 09:59:07 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_DONE: Switch 2 has
finished stack discovery
Nov 7 09:59:07 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-SWITCH_ADDED: Switch 2 has
 been added to the stack
Nov 7 09:59:14 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-ACTIVE_ELECTED: Switch 2
has been elected ACTIVE

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
```

```
San Jose, California 95134-1706


Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),

Version 03.09.12.EMD EARLY DEPLOYMENT ENGINEERING NOVA_WEEKLY BUILD, synced to
DSGS_PI2_POSTPC_FLO_DSBU7_NG3K_1105
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sun 04-Nov-12 22:53 by gereddy
License level to iosd is ipservices
```

This example displays software bootup in bundle mode:

```
switch: boot flash:cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin


Reading full image into
memory..................................................................done
Nova Bundle Image
--------------------------------------
Kernel Address : 0x6042ff38
Kernel Size : 0x318412/3245074
Initramfs Address : 0x6074834c
Initramfs Size : 0xdc08e8/14420200
Compression Format: .mzip

Bootable image at @ ram:0x6042ff38
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000,
0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "flash:cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin" uncompressed and
installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)

All packages are Digitally Signed
Starting System Services
Nov 7 09:45:49 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_START: Switch 2 is
starting stack discovery
#######################################################################################################################
Nov 7 09:47:50 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_DONE: Switch 2 has
finished stack discovery
Nov 7 09:47:50 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-SWITCH_ADDED: Switch 2 has
 been added to the stack
Nov 7 09:47:58 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-ACTIVE_ELECTED: Switch 2
has been elected ACTIVE

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
```

```
Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),
 Version 03.09.12.EMD
EARLY DEPLOYMENT ENGINEERING NOVA_WEEKLY BUILD, synced to DSGS_PI2_POSTPC_FLO_DSBU7_NG3K_1105
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sun 04-Nov-12 22:53 by gereddy
License level to iosd is ipservices
```

Related Topics

Software Boot Modes, on page 1216
Installed Boot Mode, on page 1216
Bundle Boot Mode, on page 1217

Example: Emergency Installation

This sample output is an example when the **emergency-install** boot command is initiated:

```
switch: emergency-install
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin


The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery
(tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin)...
Reading full image into memory.....................done
Nova Bundle Image
-------------------------------------
Kernel Address : 0x6042e5cc
Kernel Size : 0x318261/3244641
Initramfs Address : 0x60746830
Initramfs Size : 0xdb0fb9/14356409
Compression Format: .mzip

Bootable image at @ ram:0x6042e5cc
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000,
0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "sda9:c3850-recovery.bin" uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)



Initiating Emergency Installation of bundle
tftp://172.19.211.47/cstohs/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin


Downloading bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin...
Validating bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin...
Installing bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin...
Verifying bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin...
Package cat3k_caa-base.SSA.03.09.12.EMD.pkg is Digitally Signed
```

```
Package cat3k_caa-drivers.SSA.03.09.12.EMD.pkg is Digitally Signed
Package cat3k_caa-infra.SSA.03.09.12.EMD.pkg is Digitally Signed
Package cat3k_caa-iosd-universalk9.SSA.150-9.12.EMD.pkg is Digitally Signed
Package cat3k_caa-platform.SSA.03.09.12.EMD.pkg is Digitally Signed
Package cat3k_caa-wcm.SSA.03.09.12.EMD.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.


Booting...(use DDR clock 667 MHz)Initializing and Testing RAM +++@@@@####...++@@++@@++@@++@
```

Related Topics

Software Boot Modes, on page 1216
Installed Boot Mode, on page 1216
Bundle Boot Mode, on page 1217

Configuration Examples for Performing Switch Setup

Example: Configuring a Switch to Download Configurations from a DHCP Server

This example uses a Layer 3 SVI interface on VLAN 99 to enable DHCP-based autoconfiguration with a saved configuration:

```
Switch# configure terminal
Switch(config)# boot host dhcp
Switch(config)# boot host retry timeout 300
Switch(config)# banner config-save ^C Caution - Saving Configuration File to NVRAM May Cause
 You to No longer Automatically Download Configuration Files at Reboot^C
Switch(config)# vlan 99
Switch(config-vlan)# interface vlan 99
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch# show boot
BOOT path-list:
Config file:          flash:/config.text
Private Config file:  flash:/private-config.text
Enable Break:         no
Manual Boot:          no
HELPER path-list:
NVRAM/Config file
      buffer size:    32768
Timeout for Config
          Download:    300 seconds
Config Download
       via DHCP:       enabled (next boot: enabled)
Switch#
```

Examples: Scheduling Software Image Reload

This example shows how to reload the software on the switch on the current day at 7:30 p.m:

```
Switch# reload at 19:30
Reload scheduled for 19:30:00 UTC Wed Jun 5 2013 (in 2 hours and 25 minutes)
Proceed with reload? [confirm]
```

This example shows how to reload the software on the switch at a future time:

```
Switch# reload at 02:00 jun 20
Reload scheduled for 02:00:00 UTC Thu Jun 20 2013 (in 344 hours and 53 minutes)
Proceed with reload? [confirm]
```

Additional References For Performing Switch Setup

Related Documents

Related Topic	Document Title
Switch setup commands Boot loader commands	*System Management Command Reference (Catalyst 3850 Switches)System Management Command Reference (Cisco WLC 5700 Series)*
Pre-download feature	*System Management Configuration Guide (Cisco WLC 5700 Series)*
IOS XE DHCP configuration	*IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*
Hardware installation	*Catalyst 3850 Switch Hardware Installation Guide*
Platform-independent command references	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*
Platform-independent configuration information	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

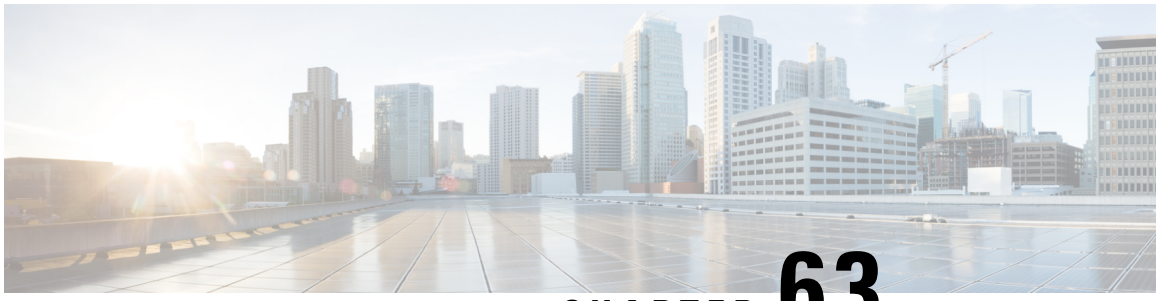
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Performing Switch Setup Configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 63

Configuring Right-To-Use Licenses

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring RTU Licenses

The following are the restrictions for configuring and using RTU licenses.

- AP count licenses can be ordered and pre-activated on your switch.
- Imaged based licenses can be upgraded. AP count licenses can be deactivated and moved between switches and controllers.
- To activate a license, you must reboot your switch after configuring the new license level. The AP-count license does not require a reboot to activate.
- An expired evaluation license can not be reactivated after reboot.
- Stack members of a switch stack must run the same license level. If the license level is different, the switch will not join the stack until it is changed and rebooted from the active switch of the stack.

- When you downgrade the license level from an image with add-on licenses to an image without add-ons, the base license level is retained after downgrade.

  When you upgrade back to the image with the add-ons, the base license level is retained but the add-ons are not activated.

- Adder AP-count licenses are installed in the factory.

Related Topics

Activating an Image Based License, on page 1241
Examples: Activating RTU Image Based Licenses, on page 1245

Information About Configuring RTU Licenses

Right-To-Use Licensing

Right-to-use (RTU) licensing allows you to order and activate a specific license type and level, and then to manage license usage on your switch. The types of licenses available to order by duration are:

- Permanent licenses—Purchased with a specific feature set with no expiration date.
- Evaluation licenses—Pre-installed on the switch and is valid for only a 90 day in-use period.

To activate a permanent or evaluation license, you are required to accept the End-User License Agreement (EULA).

A permanent license can be moved from one device to another. To activate a license, you must reboot your switch.

If you activate the evaluation license, it will expire in 90 days. An evaluation license is a manufacturing image on your switch and is not transferable to another switch. Once activated, this type of license cannot be deactivated until it expires. After your evaluation period expires, at the next reload your switch image will return to its default license and network operations are not impacted.

Related Topics

Activating an Image Based License, on page 1241
Examples: Activating RTU Image Based Licenses, on page 1245

Right-To-Use Image-Based Licenses

Right-to-use image licenses support a set of features based on a specific image-based license:

- LAN Base—Layer 2 features.
- IP Base—Layer 2 and Layer 3 features.
- IP Services—Layer 2, Layer 3, and IPv6 features. (Applicable only to switches and not controllers.)

Right-To-Use License States

After you configure a specific license type and level, you can manage your licenses by monitoring the license state.

Table 89: RTU License States

License State	Description
Active, In Use	EULA was accepted and the license is in use after device reboot.
Active, Not In Use	EULA was accepted and the switch is ready to use when the license is enabled.
Not Activated	EULA was not accepted.

Guidelines to follow when monitoring your image based license state:

- A purchased permanent license is set to *Active, In Use* state only after a switch reboot.
- If more than one license was purchased, a reboot will activate the license with the highest feature set. For instance, the IP Services license is activated and not the LAN Base license.
- Remaining licenses purchased after switch reboot, stay in **Active, Not In Use** state.

Note For the AP count license, to change the state to Active, In Use, you must first make sure that the evaluation AP count license is deactivated.

License Activation for Switch Stacks

Right-to-use licensing is supported on switch stacks. One switch in the stack is identified as the active switch and the remaining switches are standby switches. The active switch is activated with an RTU license from its active console. The license level for the standby switches in the stack can be activated at the same time.

Note A switch stack cannot contain mixed license levels. Also, the switches must be of the same platform.

To change the license level, you do not need to disconnected the new added stack member if the stack cables are connected. Use the active switch console to set the new member's license level same as active switch and reboot the new member to join the stack.

Mobility Controller Mode

AP-count licenses are used only when the switch is in Mobility Controller mode. The MC is the gatekeeper for tracking the AP-count licenses and allows an access point to join or not.

Management of AP-count licenses is performed by the switch in mobility controller mode configurable through the CLI.

Right-To-Use AP-Count Licensing

Right-to-use licensing (RTU) allows you to order and activate a specific license type, and then to manage license usage on your switch.

You can order your switch with support for a specific number of adder access point count licenses, but the total number of licenses ordered should not exceed 501000. You can also order your adder access point count licenses after receiving the switch.

For example, if you have ordered 50700 new adder licenses, you can add only those ordered adder licenses to the switch. The licenses can be added in increments of 1, but the total number of licenses added for the switch should not exceed 50 1000.

You can configure switch to manage the access point count licenses from the CLI and view the number of access points currently in use from both the CLI and GUI.

You can configure your switch to manage the access point count licenses and view the number of access points currently in use from the CLI.

The following are two different types of access point licenses:

1. Permanent licenses for the access points
    - Adder access point count license—You can purchase the adder license to increase the switch capacity at a later time. You can transfer the adder access point count license from one switch to another.

2. Evaluation licenses for the access points
    - You can activate these licenses to evaluate more access points before purchasing the licenses.
    - The maximum number of access points that can be evaluated is 50 1000.
    - The evaluation period for using the access point licenses is 90 days.
    - You can activate and deactivate the evaluation licenses from the CLI.

Related Topics

Activating an AP-Count License, on page 1242
Obtaining an Upgrade or Capacity Adder License, on page 1243
Rehosting a License, on page 1244

Right-to-Use AP-Count Evaluation Licenses

If you are considering upgrading to a license with a higher access point count, you can try an evaluation license before upgrading to a permanent version of the license. For example, if you are using a permanent license with a 50-access-point count and want to try an evaluation license with a 100-access-point count, you can try out the evaluation license for 90 days.

When an evaluation license is activated, the permanent AP-count licenses are ignored. The maximum supported licenses of 1000 access points are available for 90 days .

To prevent disruptions in operation, the switch does not change licenses when an evaluation license expires. A warning expiry message is displayed daily starting five days prior to the expiry date. After 90 days, the evaluation license expires with a warning message. You must disable the evaluation license and then purchase the permanent license.

When the switch reboots after the evaluation license expiry, the license defaults to a permanent license.

Related Topics

Activating an AP-Count License, on page 1242
Obtaining an Upgrade or Capacity Adder License, on page 1243
Rehosting a License, on page 1244

Right-To-Use Adder AP-Count Rehosting Licenses

Revoking a license from one device and installing it on another is called rehosting. You might want to rehost a license to change the purpose of a device. For example, if you want to move your Office Extend or indoor access points to a different switch, you could transfer the adder ap-count license from one switch to another.

To rehost a license, you must deactivate the adder ap-count license from one device and activate the same license on another device.

Evaluation licenses cannot be rehosted.

How to Configure RTU Licenses

Activating an Image Based License

Procedure

	Command or Action	Purpose
Step 1	**license right-to-use activate**{**ipbase** | **ipservices** | **lanbase**} {**all** | **evaluation all** } [**slot** *slot-number*] [**acceptEULA**] **Example:** `Switch# license right-to-use activate ipservices all acceptEULA`	Activates the license level. Activation can happen on all switches and also include the EULA acceptance. **Note** If you do not accept EULA, the modified configuration will not take effect after reload. The default license (or a license that was not deactivated) becomes active after reload.

Step 2	**reload** [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**]
	Example:
	`Switch# reload slot 1`
	`Proceed with reload? [confirm] y`
		Reloads a specific stack member to complete the activation process for the RTU adder AP-count license.
		Note The reminder to accept the EULA is displayed after reload if it was not accepted earlier.
		When changing license level, you are not required to save the configuration. But, it is a good practice to ensure all the configuration is stored properly before reload. Changing from a higher license level to a lower license level

	Command or Action	Purpose
		on reboot will remove CLIs that are not applicable. Ensure that all features in the lower license level that are actively used are not removed.

Step 3	**show license right-to-use usage** [**slot** *slot-number*]
	Example:
	`Switch# show license right-to-use usage`
	`Slot# License Name Type usage-duration(y:m:d) In-Use EULA`
	`1 ipservices Permanent 0 :10:27 yes yes`
	`1 ipservices Evaluation 0 :0 :0 no no`
	`1 ipbase Permanent 0 :0 :9 no yes`
	`1 ipbase Evaluation 0 :0 :0 no no`
	`1 lanbase Permanent 0 :11:12 no yes`
	`Switch#`
		Displays detailed usage information.

Related Topics

Restrictions for Configuring RTU Licenses, on page 1237
Right-To-Use Licensing, on page 1238
Monitoring and Maintaining RTU Licenses, on page 1244
Examples: Activating RTU Image Based Licenses, on page 1245

Activating an AP-Count License

Procedure

	Command or Action	Purpose
Step 1	**license right-to-use activate** {**apcount** *ap-number* **slot** *slot-num*} | **evaluation**} [**acceptEULA**] **Example:** `Switch# license right to use activate apcount 5 slot 1 acceptEULA`	Activates one or more adder AP-count licenses and immediately accepts the EULA.
Step 2	**show license right-to-use usage** [**slot** *slot-number*]	Displays detailed usage information.

	Command or Action	Purpose

	Example:
	`Switch# show license right-to-use usage`
	`Slot# License Name Type usage-duration(y:m:d) In-Use EULA`
	`1 ipservices permanent 0 :3 :29 yes yes`
	`1 ipservices evaluation 0 :0 :0 no no`
	`1 ipbase permanent 0 :0 :0 no no`
	`1 ipbase evaluation 0 :0 :0 no no`
	`1 lanbase permanent 0 :0 :0 no no`
	`1 apcount evaluation 0 :3 :11 no no`
	`1 apcount base 0 :0 :0 no yes`
	`1 apcount adder 0 :0 :17 yes yes`
	`Switch#`	

Related Topics

Monitoring and Maintaining RTU Licenses, on page 1244
Right-To-Use AP-Count Licensing, on page 1240
Right-to-Use AP-Count Evaluation Licenses, on page 1240

Obtaining an Upgrade or Capacity Adder License

You can use the capacity adder licenses to increase the number of access points supported by the switch.

Procedure

	Command or Action	Purpose
Step 1	**license right-to-use** {**activate** | **deactivate**} **apcount** {*ap-number* | **evaluation** } **slot** *slot-num* [**acceptEULA**] **Example:** `Switch# license right to use activate apcount 5 slot 2 acceptEULA`	Activates one or more adder AP-count licenses and immediately accepts the EULA.

Related Topics

Right-to-Use AP-Count Evaluation Licenses, on page 1240
Right-To-Use AP-Count Licensing, on page 1240

Rehosting a License

To rehost a license, you have to deactivate the license from one switch and then activate the same license on another switch.

Procedure

	Command or Action	Purpose

Step 1	**license right-to-use deactivate [license-level] apcount** *ap-number* **slot** *slot-num*
	Example:
	`Switch# license right-to-use deactivate apcount 1 slot 1`
	Example:
	`Switch# license right-to-use deactivate ipbase slot 1`
		Deactivates the license on one switch. The "ipbase" license level is considered as the example here.

Step 2	**license right-to-use activate [license-level] slot** *slot-num* [**acceptEULA**]
	Example:
	`Switch# license right to use activate ipbase slot 2 acceptEULA`
	Example:
	`Switch# license right-to-use activate ipbase slot 2 acceptEULA`
		Activates the license on another switch. The "ipbase" license level is considered as the example here.

Related Topics

Right-To-Use AP-Count Licensing, on page 1240
Right-to-Use AP-Count Evaluation Licenses, on page 1240

Monitoring and Maintaining RTU Licenses

Command	Purpose
show license right-to-use default	Displays the default license information.
show license right-to-use detail	Displays detailed information of all the licenses in the switch stack.
show license right-to-use eula {evaluation | permanent} show license right-to-use eula {evaluation | permanent}	Displays the end user license agreement.
show license right-to-use mismatch	Displays the license information that does not match.
show license right-to-use slot *slot-number*	Displays the license information for a specific slot in a switch stack.

Command	Purpose
show license right-to-use summary	Displays a summary of the license information on the entire switch stack.
show license right-to-use usage [**slot** *slot-number*]	Displays detailed information about usage for all licenses in the switch stack.
show switch	Displays detailed information of every member in a switch stack including the state of the license.

Related Topics

Activating an Image Based License, on page 1241
Examples: Activating RTU Image Based Licenses, on page 1245
Activating an AP-Count License, on page 1242

Configuration Examples for RTU Licensing

Examples: Activating RTU Image Based Licenses

This example shows how to activate an IP Services image license and accept the EULA for a specific slot:

```
Switch# license right-to-use activate ipservices slot 1 acceptEULA
% switch-1:stack-mgr:Reboot the switch to invoke the highest activated License level
```

This example shows how to activate a license for evaluation:

```
Switch# license right-to-use activate ipservices evaluation acceptEULA
% switch-1:stack-mgr:Reboot the switch to invoke the highest activated License level
```

Related Topics

Activating an Image Based License, on page 1241
Restrictions for Configuring RTU Licenses, on page 1237
Right-To-Use Licensing, on page 1238
Monitoring and Maintaining RTU Licenses, on page 1244

Examples: Displaying RTU Licensing Information

This example shows the consolidated RTU licensing information from the active switch on a switch stack. All of the members in the stack have the same license level. When the evaluation AP-count license is activated, the adder AP-count licenses are ignored. The maximum number of AP-count licenses are available when evaluation is enabled.

```
Switch# show license right-to-use summary

License Name       Type      Period left
```

```
---------------------------------------
 ipservices      Permanent      Lifetime
---------------------------------------

License Level In Use: ipservices
License Level on Reboot: ipservices
```

This example shows a summary of permanent and adder licenses. The evaluation AP-count license is disabled displaying the total number of activated adder AP-count licenses in the switch stack. AP-count licenses in-use mean that they are connected.

```
Switch# show license right-to-use summary

  License Name    Type          Count      Period left
------------------------------------------------------------
  ipservices     permanent      N/A         Lifetime
  apcount        base           0
  apcount        adder          40          Lifetime

------------------------------------------------------------

License Level In Use: ipservices
License Level on Reboot: ipservices eval
Evaluation AP-Count: Disabled
Total AP Count Licenses: 40
AP Count Licenses In-use: 10
AP Count Licenses Remaining: 30
```

This example shows the RTU default licenses. Default licenses are pre-installed and cannot be removed or transferred. If no license is activated the switch uses the default license, after a reboot.

```
Switch# show license right-to-use default

Slot#       License Name         Type
-------------------------------------
    1            lanbase    Permanent
-------------------------------------

Slot#       License Name         Type
-------------------------------------
    2            lanbase    Permanent
-------------------------------------

Slot#       License Name         Type
-------------------------------------
    3            lanbase    Permanent
-------------------------------------
```

This example shows the consolidated RTU licensing information of the controller. When the evaluation ap-count license is activated, the base and adder ap-count licenses are ignored. The maximum number of ap-count licenses are available when evaluation is enabled.

This example shows the RTU default licenses. Default licenses are pre-installed and cannot be removed or transferred. If no license is activated the controller uses the default license, after a reboot.

```
controller# show license right-to-use  default
Slot#    License Name    Type           Count
-----------------------------------------------------
  1        apcount         base          10
```

Example: Displaying RTU License Details

This example shows all the detailed information for the RTU licenses on slot 1:

```
Controller# show license right-to-use detail slot 1
Index 6:  License Name: apcount
          Period left: Expired
          License Type: evaluation
          License State: Active, In use
          License Count: 1000
          License Location: Slot 1
Index 7:  License Name: apcount
          Period left: Lifetime
          License Type: base
          License State: Active, Not In use
          License Count: 0
          License Location: Slot 1
Index 8:  License Name: apcount
          Period left: Lifetime
          License Type: adder
          License State: Not Activated
          License Count: 0
          License Location: Slot 1
```

Example: Displaying RTU License Mismatch

This example shows the license information of the switches in a stack and a mismatch state of a member switch. The member must match the active.

```
Switch# show switch

Switch/Stack Mac Address : 1c1d.8625.7700 - Local Mac Address
                                                 H/W   Current
Switch#   Role        Mac Address     Priority Version  State
-------------------------------------------------------------------------------
*1       Active   1c1d.8625.7700     15     V02     Ready
 2       Standby  bc16.f55c.ab80     7      V04     Ready
 3       Member   580a.2095.da00     1      V03     Lic-Mismatch
```

Note To resolve the license mismatch, first check the RTU license summary:

```
Switch# show license right-to-use
```

Then change the license level of the mismatched switched so that it is the same license level of the active switch. This example shows that the IP Base license was activated for the member switch to match the active switch.

```
Switch# license right-to-use activate ipbase slot 3 acceptEULA
```

Example: Displaying RTU Licensing Usage

This example shows the detailed licensing usage on your controller.

```
Controller# show license right-to-use usage
Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
-------------------------------------------------------------------------
1      apcount        evaluation   0 :3 :3               yes   yes
1      apcount        base         0 :0 :0               no    yes
1      apcount        adder        0 :0 :0               no    no
```

Additional References for RTU Licensing

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	*System Management Command Reference (Catalyst 3850 Switches)System Management Command Reference (Cisco WLC 5700 Series)*
RTU AP image preload feature	*System Management Configuration Guide (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

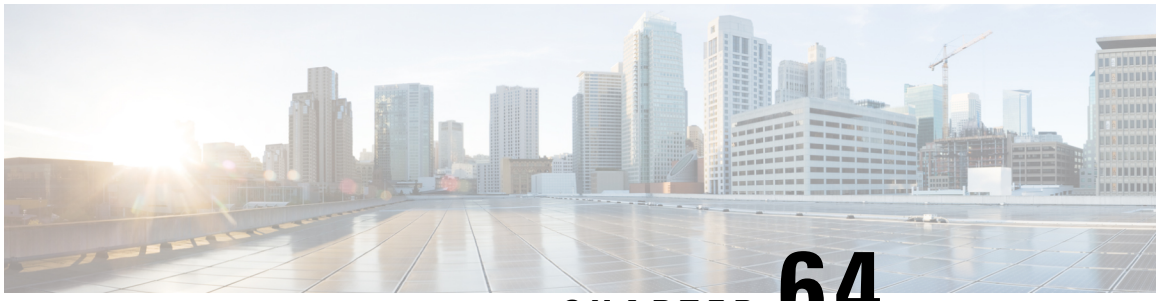
MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for RTU Licensing

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 64

Configuring Administrator Usernames and Passwords

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configuring Administrator Usernames and Passwords

You can configure administrator usernames and passwords to prevent unauthorized users from reconfiguring the switch and viewing configuration information. This section provides instructions for initial configuration and for password recovery.

You can also set administrator usernames and passwords to manage and configure one or more access points that are associated with the switch.

Strong Passwords

You can set strong administrator passwords such as encrypted passwords with ASCII keys for the administrator user for managing access points.

Use the following guidelines while creating strong passwords:

- There should be at least three of the following categories—lowercase letters, uppercase letters, and digits, and special characters.

Note Special characters are not supported for username and password for GUI login.

- The new password should not be the same as that of the associated username and the username should not be reversed.
- The characters in the password should not be repeated more than three times consecutively.
- The password should not be **cisco**, **ocsic**, **admin**, **nimda**, or any variant obtained by changing the capitalization of letters therein, or by substituting "1" "|" or "!" for i, and/or substituting "0" for "o", and/or substituting "$" for "s".
- The maximum number of characters accepted for the username and password is 32.

Encrypted Passwords

You can set three types of keys for the password:

- Randomly generated key—This key is generated randomly and it is the most secure option. To export the configuration file from one system to another, the key should also be exported.
- Static key—The simplest option is to use a fixed (static) encryption key. By using a fixed key, no key management is required, but if the key is somehow discovered, the data can be decrypted by anyone with the knowledge of that key. This is not a secure option and it is called obfuscation in the CLI.
- User defined key—You can define the key by yourself. To export the configuration file from one system to another, both systems should have the same key configured.

Note When you configure the **ap mgmtuser username** and **ap dot1x username** commands, the system encrypts the password automatically when password encryption aes is enabled and the encryption key is configured with the **key config-key password-encrypt** command. If an already-encrypted password is entered (that is, type 8), then it must be one that has been encrypted with the currently stored key. If the key of the encrypted password does not match the currently stored key, the encrypted password is rejected. In such case, you can enter the password in plain text (that is, type 0) and allow the system to encrypt it automatically.

Configuring Administrator Usernames and Passwords

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wireless security strong-password** **Example:** `Switch(config)# wireless security strong-password`	Enables strong password policy for the administrator user.
Step 3	**username** *admin-username* **password {0** *unencrypted_password* **| 7** *hidden_password* **|** *unencrypted_text***}** **Example:** `Switch(config)# username adminuser1 password 0 QZsek239@`	Specifies a username and password for an administrator. The administrator can configure the switch and view the configured information.
Step 4	**username** *admin-username* **secret {0** *unencrypted_secret_text* **| 4** *SHA256 encrypted_secret_text* **| 5** *MD5 encrypted_secret_text* **| LINE}** **Example:** `Switch(config)# username adminuser1 secret 0 QZsek239@`	Specifies the secret for the administrator.
Step 5	**ap mgmtuser username** *username* **password {0** *unencrypted password* **| 8** *AES encrypted password* **}secret {0** *unencrypted password* **| 8** *AES encrypted password* **}** **Example:** `Switch(config)# ap mgmtuser username cisco password 0 Qwci12@ secret 0 Qwci14@!`	Specifies administrator username and password for managing all of the access points configured to the switch. You can also include the secret text to perform privileged access point management. **Note** If your password is not strong enough to fulfill the strong password policy, then the password is rejected with a valid error message. For example, the following password is rejected because it is not a strong password. `Switch# ap mgmtuser username cisco password 0 abcd secret 0 1234`
Step 6	**ap dot1x username** *username* **password {0** *unencrypted password* **| 8** *AES encrypted password* **}** **Example:** `Switch(config)# ap dot1x username cisco password 0 Qwci12@`	Specifies the 802.1X username and password for managing all of the access points configured to the switch.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

	Command or Action	Purpose
Step 8	**ap name apname mgmtuser username** *username***password** *password* **secret** *secret_text* **Example:** `Switch# ap name APf0f7.55c7.7b23 mgmtuser username cisco password Qne35! secret Nzep592$`	Configures the administrator username, password, and secret text for managing a specific access point that is configured to the switch.
Step 9	**ap name apname dot1x-user** *username* **password** *password* **Example:** `Switch# ap name APf0f7.55c7.7b23 dot1x-user username cisco password Qne35!`	Configures the 802.1X username and password for a specific access point.

Example

Examples: Administrator Usernames and Passwords Configuration

This example shows how to configure administrator usernames and passwords with the strong password policy in configuration mode:

```
Switch# configure terminal
Switch(config)# wireless security strong-password
Switch(config)# username adminuser1 password 0 QZsek239@
Switch(config)# ap mgmtuser username cisco password 0 Qwci12@ secret 0 Qwci14@!
Switch(config)# ap dot1x username cisco password 0 Qwci12@
Switch# end
```

This example shows how to configure administrator usernames and passwords for an access point in global EXEC mode:

```
Switch# wireless security strong-password
Switch# ap name APf0f7.55c7.7b23 mgmtuser username cisco password Qwci12@ secret Qwci14@
Switch# ap name APf0f7.55c7.7b23 dot1x-user username cisco password Qwci12@
Switch# end
```

Additional References for Administrator Usernames and Passwords

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference Guide (Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

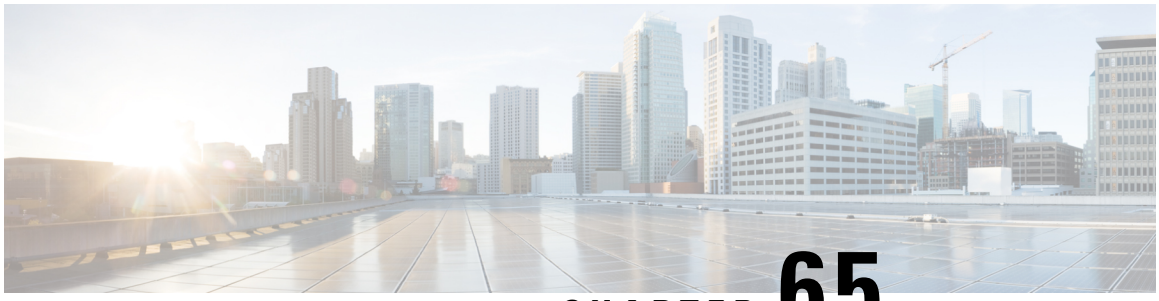
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Performing Administrator Usernames and Passwords Configuration

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 65

Configuring 802.11 parameters and Band Selection

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions on Band Selection, 802.11 Bands, and Parameters

- Band-selection enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.
- Band selection can be used only with Cisco Aironet 1140, 1250, 1260, 1550, 1600, 1800, 2600, 2800, 3500, 3600, 3700, 3800 series access points.
- Mid RSSI is not supported on Cisco Aironet 1600 Series access points.
- Band selection is not supported in Cisco Aironet 1040, OEAP 600 series access points.
- Band selection operates only on access points that are connected to a controller. A FlexConnect access point without a controller connection does not perform band selection after a reboot.

- The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.
- You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.
- It is not possible to enable or disable band selection and client load balancing globally through the controller GUI or CLI. You can, however, enable or disable band selection and client load balancing for a particular WLAN. Band selection and client load balancing are enabled globally by default.

Information About Configuring Band Selection, 802.11 Bands, and Parameters

Band Selection

Band selection enables client radios that are capable of dual-band (2.4- and 5-GHz) operation to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of three nonoverlapping channels. To prevent these sources of interference and improve overall network performance, you can configure band selection on the switch.

Band selection works by regulating probe responses to clients and it can be enabled on a per-WLAN basis. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels. In the access point, the band select table can be viewed by giving show dot11 band-select command. It can also be viewed from show cont d0/d1 | begin Lru.

Note The WMM default configuration will not be shown in **show running-config** output.

Band Selection Algorithm

The band selection algorithm affects clients that use 2.4-GHz band. Initially, when a client sends a probe request to the access point, the corresponding client probe's Active and Count values (as seen from the band select table) become 1. The algorithm functions based on the following scenarios:

- Scenario - 1: Client RSSI (as seen from **show cont d0/d1** | **begin RSSI**) is greater than both Mid-RSSI and Acceptable Client RSSI.
  - Dual band clients—No 2.4-GHz probe responses are seen at any time; 5-GHz probe responses are seen for all 5-GHz probe requests.
  - Single band (2.4-GHz) clients— 2.4-GHz probe responses are seen only after the probe suppression cycle.
  - After the client's probe count reaches the configured probe cycle count, the algorithm waits for the Age Out Suppression time and then marks the client probe's Active value as 0. Then, the algorithm is restarted.

- Scenario - 2: Client RSSI (as seen from **show cont d0/d1** | **begin RSSI**) lies between Mid-RSSI and Acceptable Client RSSI.
  - All 2.4-GHz and 5-GHz probe requests are responded without any restrictions.
  - This scenario is similar to the band select disabled.

Note The client RSSI value (seen as **sh cont d0** | **begin RSSI**) is the average of the client packets received, and the Mid-RSSI feature is the instantaneous RSSI value of the probe packets. As a result, the client RSSI is seen as weaker than the configured Mid-RSSI value (7 dB delta). The 802.11b probes from the client are suppressed to push the client to associate with the 802.11a band.

802.11 Bands

You can configure the 802.11b/g/n (2.4 GHz) and 802.11a/n/ac (5 GHz) bands for the controller to comply with the regulatory requirements in your country. By default, both 802.11b/g/n and 802.11a/n/ac are enabled.

When a controller is configured to allow only 802.11g traffic, 802.11b client devices are able to successfully connect to an access point but cannot pass traffic. When you configure the controller for 802.11g traffic only, you must mark 11g rates as mandatory.

Note The Block Acks in a Cisco 2800, 3800, 1560 APs are sent at configured mandatory data rates in Cisco WLC for 2.4 GHz radio.

802.11n Parameters

This section provides instructions for managing 802.11n access points on your network. The 802.11n devices support the 2.4- and 5-GHz bands and offer high-throughput data rates.

The 802.11n high-throughput rates are available on all 802.11n access points for WLANs using WMM with no Layer 2 encryption or with WPA2/AES encryption enabled.

The 802.11n-only access points can filter out clients without high-throughput information element on the association request. The 802.11n-only access points access points reject association requests from clients without high-throughput information element (11n).

In the 802.11n high-throughput mode, there are no 802.11a/b/g stations using the same channel. The 802.11a/b/g devices cannot communicate with the 802.11n high-throughput mode access point, where as the 802.11n-only mode access point uses 802.11a/g rates for beacons or management frames.

Note Some Cisco 802.11n APs may intermittently emit incorrect beacon frames, which can trigger false wIPS alarms. We recommend that you ignore these alarms. The issue is observed in the following Cisco 802.11n APs: 1140, 1250, 2600, 3500, and 3600.

802.11h Parameters

802.11h informs client devices about channel changes and can limit the transmit power of those client devices.

How to Configure 802.11 Bands and Parameters

Configuring Band Selection (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wireless client band-select cycle-count** *cycle_count* **Example:** `Switch(config)# wireless client band-select cycle-count 3`	Sets the probe cycle count for band select. You can enter a value between 1 and 10 for the *cycle_count* parameter.
Step 3	**wireless client band-select cycle-threshold** *milliseconds* **Example:** `Switch(config)# wireless client band-select cycle-threshold 5000`	Sets the time threshold for a new scanning cycle period. You can enter a value for threshold between 1 and 1000 for the *milliseconds* parameter.
Step 4	**wireless client band-select expire suppression** *seconds* **Example:** `Switch(config)# wireless client band-select expire suppression 100`	Sets the suppression expire to the band select. You can enter a value for suppression between 10 to 200 for the *seconds* parameter.
Step 5	**wireless client band-select expire dual-band** *seconds* **Example:** `Switch(config)# wireless client band-select expire dual-band 100`	Sets the dual band expire. You can enter a value for dual band between 10 and 300 for the *seconds* parameter.
Step 6	**wireless client band-select client-rssi** *client_rssi* **Example:** `Switch(config)# wireless client band-select client-rssi 40`	Sets the client RSSI threshold. You can enter a value for minimum dBm of a client RSSI to respond to a probe between 20 and 90 for the *client_rssi* parameter.

	Command or Action	Purpose
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Step 8	**wlan** *wlan_profile_name wlan_ID SSID_network_name* **band-select**
	Example:
	`Switch(config)# wlan wlan1 25 ssid12`
	`Switch(config-wlan)# band-select`
		Configures band selection on specific WLANs.
		You can enter a value between 1 and 512 for the *wlan_ID* parameter.
		You can enter the up to 32 alphanumeric characters for *SSID_network_name* parameter.

Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring the 802.11 Bands (CLI)

You can configure 802.11 bands and parameters.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 5ghz shutdown** **Example:** `Switch(config)# ap dot11 5ghz shutdown`	Disables the 802.11a band. **Note** You must disable the 802.11a band before configuring the 802.11a network parameters.
Step 3	**ap dot11 24ghz shutdown** **Example:** `Switch(config)# ap dot11 24ghz shutdown`	Disables the 802.11b band. **Note** You must disable the 802.11b band before configuring the 802.11b network parameters.
Step 4	**ap dot11 {5ghz | 24ghz} beaconperiod** *time_unit* **Example:** `Switch(config)# ap dot11 5ghz beaconperiod 500`	Specifies the rate at which the SSID is broadcast by the access point. The beacon interval is measured in time units (TUs). One TU is 1024 microseconds. You can configure the access point to send a beacon every 20 to 1000 milliseconds.

	Command or Action	Purpose
Step 5	**ap dot11 {5ghz | 24ghz} fragmentation** *threshold* **Example:** `Switch(config)# ap dot11 5ghz fragmentation 300`	Specifies the size at which packets are fragmented. The threshold is a value between 256 and 2346 bytes (inclusive). Specify a low number for areas where communication is poor or where there is a great deal of radio interference.

Step 6	**ap dot11 {5ghz | 24ghz} dtpc**
	Example:
	`Switch(config)# ap dot11 5ghz dtpc`
	`Switch(config)# no ap dot11 24ghz dtpc`
		Enables access points to advertise their channels and transmit the power levels in beacons, and probe responses.
		The default value is enabled. Client devices using dynamic transmit power control (DTPC) receive the channel and power level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan could rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there.
		Note On access points that run Cisco IOS software, this feature is called world mode.
		The **no** form of the command disables the 802.11a or 802.11b DTPC setting.

Step 7	**wireless client association limit** *number* **interval** *milliseconds* **Example:** `Switch(config)# wireless client association limit 50 interval 1000`	Specifies the maximum allowed clients that can be configured. You can configure a maximum number of association request on a single access point slot at a given interval. The range of association limit that you can configure is from one through 100. The association request limit interval is measured between 100 to 10000 milliseconds.
Step 8	**ap dot11 {5ghz | 24ghz} rate** *rate {disable | mandatory | supported}* **Example:** `Switch(config)# ap dot11 5ghz rate 36 mandatory`	Specifies the rate at which data can be transmitted between the controller and the client. • *disabled*—Defines that the clients specify the data rates used for communication. • *mandatory*—Defines that the clients support this data rate in order to associate to an access point on the controller. • *supported*—Any associated clients that support this data rate may communicate

	Command or Action	Purpose
		with the access point using that rate. However, the clients are not required to be able to use this rate in order to associate. • *rate*—Specifies the rate at which data is transmitted. For the 802.11a and 802.11b bands, the data is transmitted at the rate of 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps.
Step 9	**no ap dot11 5ghz shutdown** **Example:** `Switch(config)# no ap dot11 5ghz shutdown`	Enables the 802.11a band. **Note** The default value is enabled.
Step 10	**no ap dot11 24ghz shutdown** **Example:** `Switch(config)# no ap dot11 24ghz shutdown`	Enables the 802.11b band. **Note** The default value is enabled.
Step 11	**ap dot11 24ghz dot11g** **Example:** `Switch(config)# ap dot11 24ghz dot11g`	Enables or disables 802.11g network support. The default value is enabled. You can use this command only if the 802.11b band is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support.
Step 12	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Configuring the 802.11 Bands (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **802.11a/n/ac** > **Network** or **Configuration** > **Wireless** > **802.11b/g/n** > **Network** to open the Global Parameters page.

Step 2 Select the **802.11a/n/ac** (or **802.11b/g**) **Network Status** check box to enable the 802.11a or 802.11b/g band. To disable the band, unselect the check box. The default value is enabled. You can enable both the 802.11a and 802.11b/g bands.

Step 3 If you enabled the 802.11b/g band in *Step 2*, select the **802.11g Support** check box if you want to enable 802.11g network support. The default value is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support.

Step 4 Specify the period at which the SSID is broadcast by the access point by entering a value between 20 and 1000 milliseconds (inclusive) in the Beacon Period text box. The default value is 100 milliseconds.

Note The beacon period in controllers is listed in terms of milliseconds. The beacon period can also be measured in time units, where one time unit equals 1024 microseconds or 102.4 milliseconds. If a beacon interval is listed as 100 milliseconds in a controller, it is only a rounded off value for 102.4 milliseconds. Due to hardware limitation in certain radios, even though the beacon interval is, say 100 time units, it is adjusted to 102 time units, which roughly equals 104.448 milliseconds. When the beacon period is to be represented in terms of time units, the value is adjusted to the nearest multiple of 17.

Step 5 Specify the size at which packets are fragmented by entering a value between 256 and 2346 bytes (inclusive) in the Fragmentation Threshold text box. Enter a low number for areas where communication is poor or where there is a great deal of radio interference.

Step 6 Make access points advertise their channel and transmit power level in beacons and probe responses for CCX clients. Select the **DTPC Support** check box. Otherwise, unselect this check box. The default value is enabled.

Client devices using dynamic transmit power control (DTPC) receive the channel and power level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan could rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there.

Note On access points that run Cisco IOS software, this feature is called *world mode*.

Note DTPC and 801.11h power constraint cannot be enabled simultaneously.

Step 7 Specify the maximum allowed clients by entering a value between 1 to 200 in the Maximum Allowed Client text box. The default value is 200.

Step 8 Use the Data Rates options to specify the rates at which data can be transmitted between the access point and the client. These data rates are available:

- 802.11a—6, 9, 12, 18, 24, 36, 48, and 54 Mbps
- 802.11b/g—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps

For each data rate, choose one of these options:

- **Mandatory**—Clients must support this data rate in order to associate to an access point on the controller.
- **Supported**—Any associated clients that support this data rate may communicate with the access point using that rate. However, the clients are not required to be able to use this rate in order to associate.
- **Disabled**—The clients specify the data rates used for communication.

Step 9 Click **Apply**.

Step 10 Click **Save Configuration**.

Configuring 802.11n Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 {5ghz | 24ghz} dot11n** **Example:** `Switch(config)# ap dot11 5ghz dot11n`	Enables 802.11n support on the network. The **no** form of the command disables the 802.11n support on the network.
Step 3	**ap dot11 {5ghz | 24ghz} dot11n mcs tx** *rtu* **Example:** `Switch(config)# ap dot11 5ghz dot11n mcs tx 20`	Specifies the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. You can set a value from 0 through 23 for the **mcs tx** parameter. The **no** form of the command disables the MCS rates that is configured.

Step 4	**wlan***wlan_profile_name wlan_ID SSID_network_name* **wmm require**
	Example:
	`Switch(config)# wlan wlan1 25 ssid12`
	`Switch(config-wlan)# wmm require`
		Enables WMM on the WLAN and uses the 802.11n data rates that you configured.
		The **require** parameter requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

Step 5	**ap dot11 {5ghz | 24ghz} shutdown** **Example:** `Switch(config)# ap dot11 5ghz shutdown`	Disables the network.
Step 6	**{ap | no ap} dot11 {5ghz | 24 ghz} dot11n a-mpdu tx priority {all | 0-7}** **Example:** `Switch(config)# ap dot11 5ghz dot11n a-mpdu tx priority all`	Specifies the aggregation method used for 802.11n packets. Aggregation is the process of grouping packet data frames together rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU). Both A-MPDU and A-MSDU are performed in the software. You can specify the aggregation method for various types of traffic from the access point to the clients. The following table defines the priority levels (0-7) assigned per traffic type.

	Command or Action	Purpose
		Table 90: Traffic Type Priority Levels **User Priority** / **Traffic Type** 0 – Best effort 1 – Background 2 – Spare 3 – Excellent effort 4 – Controlled load 5 – Video, less than 100-ms latency and jitter 6 – Voice, less than 100-ms latency and jitter 7 – Network control You can configure each priority level independently, or you can use the all parameter to configure all of the priority levels at once. You can configure priority levels so that the traffic uses either A-MPDU transmission or A-MSDU transmission. • When you use the **ap** command along with the other options, the traffic associated with that priority level uses A-MPDU transmission. • When you use the **no ap** command along with the other options, the traffic associated with that priority level uses A-MSDU transmission. Configure the priority levels to match the aggregation method used by the clients. By default, A-MPDU is enabled for priority level 0, 4 and 5 and the rest are disabled. By default, A-MPDU is enabled for all priorities except 6 and 7.
Step 7	**no ap dot11 {5ghz | 24ghz} shutdown** **Example:** `Switch(config)# no ap dot11 5ghz shutdown`	Reenables the network.

	Command or Action	Purpose
Step 8	**ap dot11 {5ghz | 24ghz} dot11n guard-interval {any | long}** **Example:** `Switch(config)# ap dot11 5ghz dot11n guard-interval long`	Configures the guard interval for the network.
Step 9	**ap dot11 {5ghz | 24ghz} dot11n rifs rx** **Example:** `Switch(config)# ap dot11 5ghz dot11n rifs rx`	Configures the Reduced Interframe Space (RIFS) for the network.
Step 10	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring the 802.11n Parameters (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **802.11a/n/ac or 802.11b/g/n** > **High Throughput (802.11n)** to open the 802.11n/ac (5 GHz or 2.4 GHz) Throughput page.

Step 2 Select the **Enable 11n** check box to enable 802.11n support on the network. The default value is enabled.

Step 3 Select the check boxes of the desired rates to specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. These data rates, which are calculated for a 20-MHz channel width using a short guard interval, are available:

- 0 (7 Mbps)
- 1 (14 Mbps)
- 2 (21 Mbps)
- 3 (29 Mbps)
- 4 (43 Mbps)
- 5 (58 Mbps)
- 6 (65 Mbps)
- 7 (72 Mbps)
- 8 (14 Mbps)
- 9 (29 Mbps)
- 10 (43 Mbps)
- 11 (58 Mbps)

- 12 (87 Mbps)
- 13 (116 Mbps)
- 14 (130 Mbps)
- 15 (144 Mbps)
- 16 (22 Mbps)
- 17 (43 Mbps)
- 18 (65 Mbps)
- 19 (87 Mbps)
- 20 (130 Mbps)
- 21 (173 Mbps)
- 22 (195 Mbps)
- 23 (217 Mbps)
- Any associated clients that support the selected rates may communicate with the access point using those rates. However, the clients are not required to be able to use this rate in order to associate. The MCS settings determine the number of spatial streams, the modulation, the coding rate, and the data rate values that are used.

Step 4 Click **Apply**.

Step 5 Use the 802.11n data rates that you configured by enabling WMM on the WLAN as follows:

a) Choose **WLANs** to open the WLANs page.
b) Click the ID number of the WLAN for which you want to configure WMM mode.
c) When the WLANs > Edit page appears, choose the **QoS** tab to open the WLANs > Edit (Qos) page.
d) From the WMM Policy drop-down list, choose **Required** or **Allowed** to require or allow client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

   If you choose **Allowed**, devices that cannot support WMM can join the WLAN but will not benefit from the 802.11n rates.

e) Click **Apply**.

Step 6 Click **Save Configuration**.

Note To determine if an access point supports 802.11n, look at the 11n Supported text box on either the 802.11a/n/ac (or 802.11b/g/n) Cisco APs > Configure page or the 802.11a/n/ac (or 802.11b/g/n) AP Interfaces > Details page.

Configuring 802.11h Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap dot11 5ghz shutdown** **Example:** `Switch(config)# ap dot11 5ghz shutdown`	Disables the 802.11a network.
Step 2	**{ap | no ap} dot11 5ghz channelswitch mode** *switch_mode* **Example:** `Switch(config)# ap dot11 5ghz channelswitch mode 0`	Enables or disables the access point to announce when it is switching to a new channel. You can enter a 0 or 1 for the **channelswitch** parameter to specify whether transmissions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled.
Step 3	**ap dot11 5ghz power-constraint** *value* **Example:** `Switch(config)# ap dot11 5ghz power-constraint 200`	Configures the 802.11h power constraint value in a range from zero through 255. The default value for the value parameter is 3 dB.
Step 4	**no ap dot11 5ghz shutdown** **Example:** `Switch(config)# no ap dot11 5ghz shutdown`	Reenables the 802.11a network.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring the 802.11h Parameters (GUI)

Procedure

Step 1 Disable the 802.11 band as follows:

a) Choose **Configuration** > **Wireless > 802.11a/n/ac > Network** to open the 802.11a/n/ac Global Parameters page.
b) Unselect the **802.11a Network Status** check box.
c) Click **Apply**.

Step 2 Choose **Configuration** > **Wireless > 802.11a/n/ac > DFS (802.11h)** to open the 802.11h Global Parameters page.

Step 3 In the Power Constraint area, enter the local power constraint. The valid range is between 0 dBm and 30 dBm.

Step 4 In the Channel Switch Announcement area, enter the channel switch announcement mode. You can enter a value of either 1 or 0.

Step 5 Click **Apply**.

Step 6 Reenable the 802.11a band as follows:

a) Choose **Wireless > 802.11a/n/ac > Network** to open the 802.11a/n/ac Global Parameters page.

b) Select the **802.11a Network Status** check box.

c) Click **Apply**.

Step 7 Click **Save Configuration**.

Monitoring Configuration Settings for Band Selection, 802.11 Bands, and Parameters

Monitoring Configuration Settings Using Band Selection and 802.11 Bands Commands

This section describes the new commands for band selection and 802.11 bands.

The following commands can be used to monitor band selection, and 802.11 bands and parameters the switch.

Table 91: Monitoring Configuration Settings Using Band Selection and 802.11 Bands Commands

Command	Purpose
show ap dot11 5ghz network	Displays 802.11a bands network parameters, 802.11a operational rates, 802.11n MCS settings, and 802.11n status information.
show ap dot11 24ghz network	Displays 802.11b bands network parameters, 802.11b/g operational rates, 802.11n MCS settings, and 802.11n status information.
show wireless dot11h	Displays 802.11h configuration parameters.
show wireless band-select	Displays band select configuration settings.

Example: Viewing the Configuration Settings for 5-GHz Band

```
Switch# show ap dot11 5ghz network
802.11a Network : Enabled
11nSupport : Enabled
  802.11a Low Band : Enabled
  802.11a Mid Band : Enabled
  802.11a High Band : Enabled

802.11a Operational Rates
  802.11a 6M : Mandatory
  802.11a 9M : Supported
```

```
    802.11a 12M : Mandatory
    802.11a 18M : Supported
    802.11a 24M : Mandatory
    802.11a 36M : Supported
    802.11a 48M : Supported
    802.11a 54M : Supported
  802.11n MCS Settings:
    MCS 0 : Supported
    MCS 1 : Supported
    MCS 2 : Supported
    MCS 3 : Supported
    MCS 4 : Supported
    MCS 5 : Supported
    MCS 6 : Supported
    MCS 7 : Supported
    MCS 8 : Supported
    MCS 9 : Supported
    MCS 10 : Supported
    MCS 11 : Supported
    MCS 12 : Supported
    MCS 13 : Supported
    MCS 14 : Supported
    MCS 15 : Supported
    MCS 16 : Supported
    MCS 17 : Supported
    MCS 18 : Supported
    MCS 19 : Supported
    MCS 20 : Supported
    MCS 21 : Supported
    MCS 22 : Supported
    MCS 23 : Supported
  802.11n Status:
    A-MPDU Tx:
      Priority 0 : Enabled
      Priority 1 : Disabled
      Priority 2 : Disabled
      Priority 3 : Disabled
      Priority 4 : Enabled
      Priority 5 : Enabled
      Priority 6 : Disabled
      Priority 7 : Disabled
    A-MSDU Tx:
      Priority 0 : Enabled
      Priority 1 : Enabled
      Priority 2 : Enabled
      Priority 3 : Enabled
      Priority 4 : Enabled
      Priority 5 : Enabled
      Priority 6 : Disabled
      Priority 7 : Disabled
  Guard Interval : Any
    Rifs Rx : Enabled
  Beacon Interval : 100
  CF Pollable mandatory : Disabled
  CF Poll Request Mandatory : Disabled
  CFP Period : 4
  CFP Maximum Duration : 60
  Default Channel : 36
  Default Tx Power Level : 1
  DTPC Status : Enabled
  Fragmentation Threshold : 2346
  Pico-Cell Status : Disabled
  Pico-Cell-V2 Status : Disabled
  TI Threshold : 0
```

```
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type check : default-wmm
Call Admision Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP Codec Type : CODEC_TYPE_G711
  SIP call bandwidth : 64
  SIP call bandwith sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

Example: Viewing the Configuration Settings for 24-GHz Band

```
Switch# show ap dot11 24ghz network
802.11b Network : Enabled
11gSupport : Enabled
11nSupport : Enabled

  802.11b/g Operational Rates
  802.11b 1M : Mandatory
  802.11b 2M : Mandatory
  802.11b 5.5M : Mandatory
  802.11g 6M : Supported
  802.11g 9M : Supported
  802.11b 11M : Mandatory
  802.11g 12M : Supported
  802.11g 18M : Supported
  802.11g 24M : Supported
  802.11g 36M : Supported
  802.11g 48M : Supported
  802.11g 54M : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
  MCS 10 : Supported
  MCS 11 : Supported
  MCS 12 : Supported
  MCS 13 : Supported
  MCS 14 : Supported
  MCS 15 : Supported
  MCS 16 : Supported
  MCS 17 : Supported
```

```
  MCS 18 : Supported
  MCS 19 : Supported
  MCS 20 : Supported
  MCS 21 : Supported
  MCS 22 : Supported
  MCS 23 : Supported
802.11n Status:
  A-MPDU Tx:
    Priority 0 : Enabled
    Priority 1 : Disabled
    Priority 2 : Disabled
    Priority 3 : Disabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  A-MSDU Tx:
    Priority 0 : Enabled
    Priority 1 : Enabled
    Priority 2 : Enabled
    Priority 3 : Enabled
    Priority 4 : Enabled
    Priority 5 : Enabled
  Priority 6 : Disabled
    Priority 7 : Disabled
  Guard Interval : Any
  Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable Mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 11
Default Tx Power Level : 1
DTPC Status : true
Call Admission Limit : 105
G711 CU Quantum : 15
ED Threshold : -50
Fragmentation Threshold : 2346
PBCC Mandatory : Disabled
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
RTS Threshold : 2347
Short Preamble Mandatory : Enabled
Short Retry Limit : 7
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type : default-wmm
Call Admision Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP Codec Type : CODEC_TYPE_G711
  SIP call bandwidth : 64
  SIP call bandwith sample-size : 20
Video AC
```

```
Video AC - Admission control (ACM) : Disabled
Video max RF bandwidth : Infinite
Video reserved roaming bandwidth : 0
```

Example: Viewing the status of 802.11h Parameters

```
Switch# show wireless dot11h
Power Constraint: 0
Channel Switch: 0
Channel Switch Mode: 0
```

Example: Verifying the Band Selection Settings

The following example displays band select configuration:

```
Switch# show wireless band-select

Band Select Probe Response   : per WLAN enabling
Cycle Count                  : 2
Cycle Threshold (millisec)   : 200
Age Out Suppression (sec)    : 20
Age Out Dual Band (sec)      : 60
Client RSSI (dBm)            : -80
Client Mid RSSI (dBm)        : -80
```

Configuration Examples for Band Selection, 802.11 Bands, and Parameters

Examples: Band Selection Configuration

This example shows how to set the probe cycle count and time threshold for a new scanning cycle period for band select:

```
Switch# configure terminal
Switch(config)# wireless client band-select cycle-count 3
Switch(config)# wireless client band-select cycle-threshold 5000
Switch(config)# end
```

This example shows how to set the suppression expire to the band select:

```
Switch# configure terminal
Switch(config)# wireless client band-select expire suppression 100
Switch(config)# end
```

This example shows how to set the dual band expire for the band select:

```
Switch# configure terminal
Switch(config)# wireless client band-select expire dual-band 100
Switch(config)# end
```

This example shows how to set the client RSSI threshold for the band select:

```
Switch# configure terminal
Switch(config)# wireless client band-select client-rssi 40
Switch(config)# end
```

This example shows how to configure band selection on specific WLANs:

```
Switch# configure terminal
Switch(config)# wlan wlan1 25 ssid12
Switch(config-wlan)# band-select
Switch(config)# end
```

Examples: 802.11 Bands Configuration

This example shows how to configure 802.11 bands using beacon interval, fragmentation, and dynamic transmit power control:

```
Switch# configure terminal
Switch(config)# ap dot11 5ghz shutdown
Switch(config)# ap dot11 24ghz shutdown
Switch(config)# ap dot11 5ghz beaconperiod 500
Switch(config)# ap dot11 5ghz fragmentation 300
Switch(config)# ap dot11 5ghz dtpc
Switch(config)# wireless client association limit 50 interval 1000
Switch(config)# ap dot11 5ghz rate 36 mandatory
Switch(config)# no ap dot11 5ghz shutdown
Switch(config)# no ap dot11 24ghz shutdown
Switch(config)# ap dot11 24ghz dot11g
Switch(config)#end
```

Examples: 802.11n Configuration

This example shows how to configure 802.11n parameters for 5-GHz band using aggregation method:

```
Switch# configure terminal
Switch(config)# ap dot11 5ghz dot11n
Switch(config)# ap dot11 5ghz dot11n mcs tx 20
Switch(config)# wlan wlan1 25 ssid12
Switch(config-wlan)# wmm require\
Switch(config-wlan)# exit
Switch(config)# ap dot11 5ghz shutdown
Switch(config)# ap dot11 5ghz dot11n a-mpdu tx priority all
Switch(config)# no ap dot11 5ghz shutdown
Switch(config)#exit
```

This example shows how to configure the guard interval for 5-GHz band:

```
Switch# configure terminal
Switch(config)# ap dot11 5ghz dot11n
Switch(config)# ap dot11 5ghz dot11n mcs tx 20
Switch(config)# wlan wlan1 25 ssid12
Switch(config-wlan)# wmm require\
Switch(config-wlan)# exit
```

```
Switch(config)# no ap dot11 5ghz shutdown
Switch(config)# ap dot11 5ghz dot11n guard-interval long
Switch(config)#end
```

This example shows how to configure the RIFS for 5-GHz band:

```
Switch# configure terminal
Switch(config)# ap dot11 5ghz dot11n
Switch(config)# ap dot11 5ghz dot11n mcs tx 20
Switch(config)# wlan wlan1 25 ssid12
Switch(config-wlan)# wmm require\
Switch(config-wlan)# exit
Switch(config)# ap dot11 5ghz shutdown
Switch(config)# ap dot11 5ghz dot11n rifs rx
Switch(config)#end
```

Examples: 802.11h Configuration

This example shows how to configure the access point to announce when it is switching to a new channel using restriction transmission:

```
Switch# configure terminal
Switch(config)# ap dot11 5ghz shutdown
Switch(config)# ap dot11 5ghz channelswitch mode 0
Switch(config)# no ap dot11 5ghz shutdown
Switch(config)#end
```

This example shows how to configure the 802.11h power constraint for 5-GHz band:

```
Switch# configure terminal
Switch(config)# ap dot11 5ghz shutdown
Switch(config)# ap dot11 5ghz power-constraint 200
Switch(config)# no ap dot11 5ghz shutdown
Switch(config)#end
```

Additional References for 802.11 Parameters and Band Selection

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

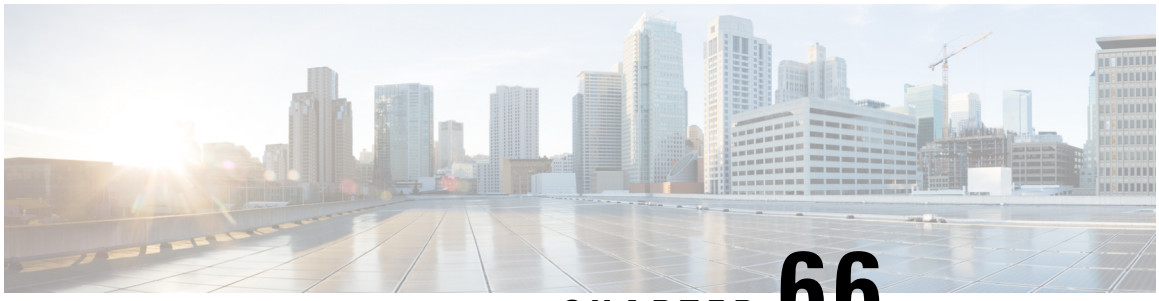
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Performing 802.11 parameters and Band Selection Configuration

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 66

Configuring Aggressive Load Balancing

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Aggressive Load Balancing

- You can configure aggressive load balancing only from the command-line interface.
- Aggressive load balancing is disabled by default, you must enable it manually.
- You can enable load balancing either separately or together with the band select configurations.
- When the band select is enabled on the dual-band clients, the load balancing parameter selects only the lowest load radio from 5-GHz radios. For the 2.4-GHz clients, there is no probe information of the client on 5 GHz and therefore the load balancing algorithm can only be selected between radio on 2.4 GHz.
- You can operate load balancing of clients between access points on the same switch but not for the clients between access points on the different switch.

- The load balancing uses an existing association denial mechanism based on the number of client on the radio and the band select is implemented by the distributed probe response suppression on the access point only.

Information for Configuring Aggressive Load Balancing Parameters

Aggressive Load Balancing

Enabling aggressive load balancing on the controller allows lightweight access points to load balance wireless clients across access points. You can enable aggressive load balancing using the controller.

When a wireless client attempts to associate to a lightweight access point, association response packets are sent to the client with an 802.11 response packet including status code 17. The code 17 indicates that the AP is busy. The AP does not respond with an association response bearing 'success' if the AP threshold is not met, and with code 17 (AP busy) if the AP utilization threshold is exceeded, and another less busy AP heard the client request.

For example, if the number of clients on AP1 is more than the number of clients on AP2 plus the load-balancing window, then AP1 is considered to be busier than AP2. When a client attempts to associate to AP1, it receives an 802.11 response packet with status code 17, indicating that the access point is busy, and the client attempts to associate to a different access point.

You can configure the controller to deny client associations up to 10 times (if a client attempted to associate 11 times, it would be allowed to associate on the 11th try). You can also enable or disable load balancing on a particular WLAN, which is useful if you want to disable load balancing for a select group of clients (such as time-sensitive voice clients).

Note Voice Client does not authenticate when delay is configured more than 300 ms. To avoid this configure a Central-Auth, Local Switching WLAN with CCKM, configure a Pagent Router between AP and WLC with a delay of 600 ms (300 ms UP and 300 ms DOWN and try associating the voice client

The maximum number of client associations that the access points can support is dependent upon the following factors:

- The maximum number of client associations differs for lightweight and autonomous Cisco IOS access points.
- There may be a limit per radio and an overall limit per AP.
- AP hardware (the 16-MB APs have a lower limit than the 32-MB and higher APs)

The Client Association Limits for Lightweight Access Points are as follows:

- For 16-MB APs, the limit is 128 clients per AP. This limit is applicable to 1100 and 1200 series APs.
- For 32-MB and higher APs, there is no per-AP limit.

The maximum Client Association Limits per-radio for all of the Cisco IOS APs is 200 associations.

Note With 32-MB and higher lightweight Cisco IOS APs, with two radios, up to 200 + 200 = 400 associations are supported.

The maximum Client Association Limits per Autonomous Cisco IOS access point is around 80 to 127 clients per AP. This number varies depending on the following factors:

- AP model (whether it is 16 MB or 32 MB or higher)
- Cisco IOS software release
- Hardware configuration (two radios use more memory than one)
- Enabled features (WDS functionality in particular)

The per-radio limit is about 200 associations. One association will likely hit the per-AP limit first. Unlike Cisco Unified Wireless Network, autonomous Cisco IOS supports per-SSID/per-AP association limits. This limit is configured using the max-associations CLI, under dot11 SSID. The maximum number is 255 associations (which is also the default number).

Note For a FlexConnect AP the association is locally handled. The load-balancing decisions are taken at the Cisco WLC. A FlexConnect AP initially responds to the client before knowing the result of calculations at the Cisco WLC. Load-balancing doesn't take effect when the FlexConnect AP is in standalone mode.

FlexConnect AP does not send (re)association response with status 17 for Load-Balancing as Local mode APs do; instead, it first sends (re)association with status 0 (success) and then deauth with reason 5.

How to Configure Aggressive Load Balancing

Configuring Aggressive Load Balancing

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wireless load-balancing window** *client-count* **Example:** `Switch(config)# wireless load-balancing window 1`	Sets the client window for aggressive load balancing. You can enter a value between 0 and 20 for the *client_count* parameter.

	Command or Action	Purpose
Step 3	**wireless load-balancing denial** *denial-count* **Example:** `Switch(config)# wireless load-balancing denial-count 1`	Sets the denial count for load balancing. You can enter a value between 0 and 10 for the *denial_count* parameter.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Step 5	**wlan** *wlan_profile_name wlan_ID SSID_network_name* **load-balance**
	Example:
	`Switch(config)# wlan wlan1 25 ssid12`
	`Switch(config-wlan)# load-balance`
		Enables or disables aggressive load balancing on specific WLANs.
		You can enter a value between 1 and 512 for the *wlan_ID* parameter.
		You can enter the up to 32 alphanumeric characters for *SSID_network_name* parameter.

Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Monitoring Aggressive Load Balancing

This section describes the new command for aggressive load balancing.

The following command can be used to monitor aggressive load balancing on the switch.

Table 92: Monitoring Aggressive Load Balancing Command

Command	Purpose
show wireless load-balancing	Displays the status of the load-balancing feature.

Examples: Aggressive Load Balancing Configuration

This example shows how to configure the load balancing denial count:

```
Switch# configure terminal
Switch(config)# wireless load-balancing denial-count 1
Switch(config)# end
Switch# show wireless load-balancing
```

This example shows how to configure the client window for aggressive load balancing:

```
Switch# configure terminal
Switch(config)# wireless load-balancing window 1
Switch(config)# end
Switch# show wireless load-balancing
```

This example shows how to configure load balancing on specific WLAN:

```
Switch# configure terminal
Switch(config)# wlan wlan1 25 ssid12
Switch(config-wlan)# load-balance
Switch(config)# end
Switch# show wireless load-balancing
```

Additional References for Aggressive Load Balancing

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

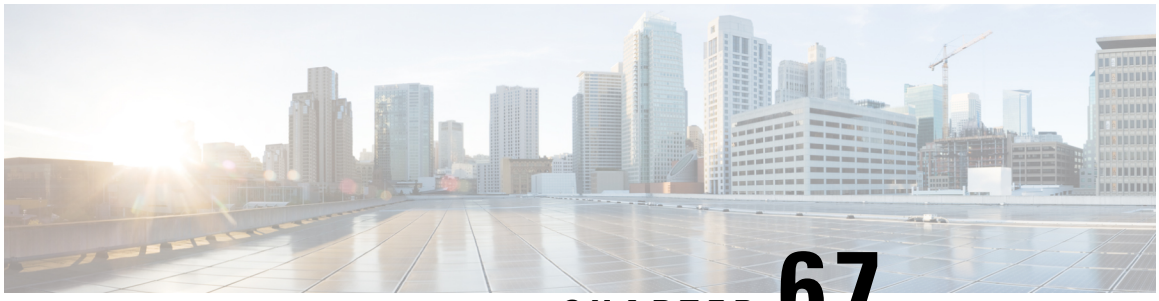
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Performing Aggressive Load Balancing Configuration

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 67

Configuring Client Roaming

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring Client Roaming

The following are the restrictions that you should be aware while configuring client roaming:

- Cisco Compatible Extensions (CCX) support is enabled automatically for every WLAN on the switch and cannot be disabled. The switch stores the CCX version of the client in its client database and uses it to generate and respond to CCX frames appropriately. Clients must support CCXv4 or v5 (or CCXv2 for access point assisted roaming) to utilize these roaming enhancements.
- Client roaming between 600 Series Access points is not supported.

Information About Client Roaming

The controllers deliver high-end wireless services to the clients roaming across wireless network. Now, the wireless services are integrated with the switches, thus delivering a value-added Cisco unified new mobility

architecture. This unified architecture enables client-roaming services to both wireless and wired clients with seamless, fast- roaming services.

The new mobility architecture supports fast client roaming services using logical categorization of network into Mobility Domains (MDs), Mobility Groups (MGs), Mobility Subdomains (MSDs), and Switch Peer Groups (SPGs) using systems such as Mobility Oracle (MO), Mobility Controller (MC), and Mobility Agent (MA).

- A **Mobility Domain** is the entire domain across which client roaming is supported. It is a collection of mobility groups. For example, a campus network can be considered as a mobility domain.
- A **Mobility Group** is a collection of mobility subdomains across which fast roaming is supported. The mobility group can be one or more buildings within a campus across which frequent roaming is supported.
- A **Mobility Subdomain** is an autonomous portion of the mobility domain network. Each mobility subdomain contains one mobility controller (MC) and a collection of SPGs. A subdomain is equivalent to an 802.11r key domain.
- A **Switch Peer Group** is a collection of mobility agents.
- The **Mobility Oracle** acts as the point of contact for mobility events that occur across mobility subdomains. The mobility oracle also maintains a local database of each client in the entire mobility domain, their home and current subdomain. There is only one MO for an entire mobility domain. The Cisco WLC 5700 Series Controllers or Cisco Unified Wireless Networking Solution controller can act as MO.
- The **Mobility Controller** provides mobility management services for inter-SPG roaming events. The MC sends the configuration like SPG name and SPG peer member list to all of the mobility agents under its subdomain. The Cisco WLC 5700 Series Controllers, Cisco Catalyst 3850 Switch, or Cisco Unified Wireless Networking Solution controller can act as MC. The MC has MC functionality and MA functionality that is running internally into it.
- The **Mobility Agent** is the component that maintains client mobility state machine for a mobile client. All APs are connected to the mobility agent.

The New mobility architecture supports seamless roaming in the following scenarios:

- Intra-switch roaming—The client roaming between APs managed by same mobility agent.
- Intra-SPG roaming—The client roaming between mobility agents in the same SPG.
- Inter-SPG, Intra-subdomain roaming—The client roaming between mobility agents in different SPGs within the same subdomain.
- Inter-subdomain roaming—The client roaming between mobility agents across a subdomain.

Fast Roaming

New mobility architecture supports fast roaming when clients roam within a mobility group by eliminating the need for full authentication. Security polices should be same across the switches for fast roaming.

Local, anchor, foreign MAs and MCs

When a client joins an MA initially and its point of attachment has not changed, that MA is referred as local or associated MA. The MC to which this MA is associated is referred as local or associated MC.

When a client roams between two MAs, the MA to which the client was previously associated is the anchor MA (point of attachment) and the MA to which the client is currently associated is the foreign or associated

MA (point of presence). The MCs to which these MAs are associated are referred as anchor, foreign, or associated MCs, respectively.

Inter-Subnet Roaming

Multiple-controller deployments support client roaming across access points managed by controllers in the same mobility group on different subnets. This roaming is transparent to the client because the session is sustained and a tunnel between the controllers allows the client to continue using the same DHCP-assigned or client-assigned IP address as long as the session remains active. The tunnel is torn down, and the client must reauthenticate when the client sends a DHCP Discover with a 0.0.0.0 client IP address or a 169.254.*.* client auto-IP address or when the operator-set user timeout is exceeded.

Voice-over-IP Telephone Roaming

802.11 voice-over-IP (VoIP) telephones actively seek out associations with the strongest RF signal to ensure the best quality of service (QoS) and the maximum throughput. The minimum VoIP telephone requirement of 20-millisecond or shorter latency time for the roaming handover is easily met by the Cisco Wireless solution, which has an average handover latency of 5 or fewer milliseconds when open authentication is used. This short latency period is controlled by controllers rather than allowing independent access points to negotiate roaming handovers.

The Cisco Wireless solution supports 802.11 VoIP telephone roaming across lightweight access points managed by controllers on different subnets, as long as the controllers are in the same mobility group. This roaming is transparent to the VoIP telephone because the session is sustained and a tunnel between controllers allows the VoIP telephone to continue using the same DHCP-assigned IP address as long as the session remains active. The tunnel is torn down, and the VoIP client must reauthenticate when the VoIP telephone sends a DHCP Discover with a 0.0.0.0 VoIP telephone IP address or a 169.254.*.* VoIP telephone auto-IP address or when the operator-set user timeout is exceeded.

CCX Layer 2 Client Roaming

The controller supports five CCX Layer 2 client roaming enhancements:

- Access point assisted roaming—This feature helps clients save scanning time. When a CCXv2 client associates to an access point, it sends an information packet to the new access point listing the characteristics of its previous access point. Roaming time decreases when the client recognizes and uses an access point list built by compiling all previous access points to which each client was associated and sent (unicast) to the client immediately after association. The access point list contains the channels, BSSIDs of neighbor access points that support the client's current SSID(s), and time elapsed since disassociation.
- Enhanced neighbor list—This feature focuses on improving a CCXv4 client's roam experience and network edge performance, especially when servicing voice applications. The access point provides its associated client information about its neighbors using a neighbor-list update unicast message.
- Enhanced neighbor list request (E2E)—The End-2-End specification is a Cisco and Intel joint program that defines new protocols and interfaces to improve the overall voice and roaming experience. It applies only to Intel clients in a CCX environment. Specifically, it enables Intel clients to request a neighbor list at will. When this occurs, the access point forwards the request to the controller. The controller receives the request and replies with the current CCX roaming sublist of neighbors for the access point to which the client is associated.

Note To see whether a particular client supports E2E, choose **Wireless** > **Clients** on the controller GUI, click the **Detail** link for the desired client, and look at the E2E Version text box in the Client Properties area.

- Roam reason report—This feature enables CCXv4 clients to report the reason why they roamed to a new access point. It also allows network administrators to build and monitor a roam history.
- Directed roam request—This feature enables the controller to send directed roam requests to the client in situations when the controller can better service the client on an access point different from the one to which it is associated. In this case, the controller sends the client a list of the best access points that it can join. The client can either honor or ignore the directed roam request. Non-CCX clients and clients running CCXv3 or below must not take any action. No configuration is required for this feature.

How to Configure Layer 2 or Layer 3 Roaming

Configuring Layer 2 or Layer 3 Roaming

Before you begin

To configure the mobility agent for Layer 2 or Layer 3 roaming, the following requisites should be considered:

- SSID and security polices should be same across MAs for Layer 2 and Layer 3 roaming.
- Client VLAN ID should be same for Layer 2 roaming and different for Layer 3 roaming.
- Bridge domain ID and client VLAN IDs should be same for Layer 2 roaming. Either one or both of the bridge domain ID and client VLAN ID should be different for Layer 3 roaming.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan_profile_name wlan_ID SSID_network_name* **Example:** `Switch(config)#wlan wlan1`	Enters WLAN configuration mode.
Step 3	**no mobility anchor sticky** **Example:** `Switch(config-wlan)#no mobility anchor sticky`	(Optional) Disables Layer 2 anchoring.

	Command or Action	Purpose
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring CCX Client Roaming Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 {5ghz | 24ghz} l2roam rf-params** {**default | custom** *min-rssi roam-hyst scan-thresh trans-time*} **Example:** `Switch#ap dot11 5ghz l2roam rf-params custom -80`	Configures CCX Layer 2 client roaming parameters. To choose the default RF parameters, enter the **default** option. To fine-tune the RF parameters that affect client roaming, enter the **custom** option and then enter any one of the following options: • Minimum RSSI—Indicates minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point. If the client's average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached. You can configure the minimum RSSI range from –50 through –90 dBm and the default value is –85 dBm. • Hysteresis—Indicates how much greater the signal strength of a neighboring access point must be for the client to roam to it. This parameter is intended to reduce the amount of roaming between access points if the client is physically located on or near the border between two access points.

	Command or Action	Purpose
		You can configure the hysteresis range from 3 through 20 dB and the default is 3 dB. • Scan Threshold—Indicates a minimum RSSI that is allowed before the client should roam to a better access point. When the RSSI drops below the specified value, the client must be able to roam to a better access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when the RSSI is below the threshold. You can configure the RSSI range from –50 through –90 dBm and the default value is –72 dBm. • Transition Time—Indicates the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client's associated access point is below the scan threshold. The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points. You can configure the time period in the range from 1 through 5 seconds and the default time is 5 seconds.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Example

Configuring Mobility Oracle

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wireless mobility oracle** **Example:** `Switch(config)# wireless mobility oracle`	Enables mobility oracle on the controller.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Example

Configuring Mobility Controller

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wireless mobility controller** **Example:** `Switch(config)# wireless mobility controller`	Enables wireless mobility controller.
Step 3	**wireless mobility controller peer-group** *switch-peer-group-name* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1`	Configures a switch peer group name. You can enter up to 31 case-sensitive ASCII printable characters for the group name. Spaces are not allowed in mobility group. **Note** The **No** form of the command deletes the switch peer group.

	Command or Action	Purpose
Step 4	**wireless mobility controller peer-group** *switch-peer-group-name* **member ip** *ip-address* {**public-ip** *public-ip-address*} **Example:** `Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.0.0.1`	Adds a mobility group member to a switch peer group. **Note** The **No** form of the command deletes the member from the switch peer group.
Step 5	**wireless mobility controller peer-group** *switch-peer-group-name* **multicast** **Example:** `Switch(config)# wireless mobility controller peer-group SPG1 multicast`	Configures the multicast mode within a switch peer group.
Step 6	**wireless mobility controller peer-group** *switch-peer-group-name* **multicast ip** *peer-group-multicast-ip-addr* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1 multicast ip 10.0.0.4`	Configures the multicast IP address for a switch peer group. **Note** The **No** form of the command deletes the multicast IP for the switch peer group.
Step 7	**wireless mobility controller peer-group***switch-peer-group-name* **bridge-domain-id** *id* **Example:** `Switch(config)# wireless mobility controller peer-group SPG bridge-domain-id 10.0.0.5`	Configures the bridge domain ID for a switch peer group. The default is zero. **Note** The **No** form of command sets the bridge domain ID to the default value.
Step 8	**wireless mobility group member ip** *ip-address* [**public-ip** *public-ip-address*] [**group** *group-name*] **Example:** `Switch(config)# wireless mobility group member ip 10.0.0.1`	Adds a mobility group member. **Note** The **No** form of the command removes the member from the group. The default group name is the group name of MC.
Step 9	**wireless mobility dscp** *value* **Example:** `Switch(config)# wireless mobility dscp 46`	Sets the DSCP value for mobility control packet. You can configure the DSCP value in a range from 0 through 63. The default value is 46.
Step 10	**wireless mobility group keepalive** {*count* | *interval*}	Configures the wireless mobility group keepalive count which is the number of keepalive retries before a member status is

	Command or Action	Purpose
	Example: `Switch(config)# wireless mobility group keepalive count`	termed DOWN and keepalive interval which is interval between two keepalives.
Step 11	**wireless mobility group name** *name* **Example:** `Switch(config)# wireless mobility group name group1`	Specifies the case sensitive wireless mobility group name which can be ASCII printable string up to 31 characters.
Step 12	**wireless mobility oracle ip***mo-ip-address* **Example:** `Switch(config)# wireless mobility oracle ip 10.0.0.5`	Configures the mobility oracle IP address.
Step 13	**wireless management interface** *interface-name* **Example:** `Switch(config)# wireless management interface Vlan21`	Configures the wireless management interface.
Step 14	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Example

Configuring Mobility Agent

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wireless mobility controller ip** *ip-address* **Example:** `Switch(config)# wireless mobility controller ip 10.10.10.20`	Sets the IP address of the mobility controller.
Step 3	**wireless mobility load-balance** **Example:** `Switch(config)# wireless mobility load-balance`	Configures wireless mobility load balancing.

	Command or Action	Purpose
Step 4	**wireless mobility load-balance threshold** *threshold -value* **Example:** `Switch(config)# wireless mobility load-balance threshold 100`	Configures the number of clients that can be local or anchored on the MA. You can configure the threshold value in a range from 100 to 2000. The default value is 1000.
Step 5	**wireless management interface** *interface-name* **Example:** `Switch(config)# wireless management interface Vlan21`	Configures wireless management interface for the mobility agent.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Monitoring Client Roaming Parameters

This section describes the new commands for the client parameters.

The following commands can be used to monitor the client roaming parameters on the switch.

Table 93: Monitoring Client Roaming Parameters Commands

Command	Purpose
show ap dot11 {5ghz | 24ghz} l2roam rf-param	Displays the current RF parameters configured for client roaming for the 802.11a or 802.11b/g network.
show ap dot11 {5ghz | 24ghz} l2roam statistics	Displays the CCX Layer 2 client roaming statistics for the 802.11a or 802.11b/g network.
show ap dot11 {5ghz | 24ghz} l2roam mac-address *mac-address* **statistics**	Displays the CCX Layer 2 client roaming statistics for a particular access point.

Monitoring Mobility Configurations

This section describes the new commands for monitoring mobility configurations.

The following command can be used to monitor mobility configurations on the Mobility Oracle, Mobility Controller, and Mobility Agent.

Table 94: Monitoring Mobility Configuration Commands on the Mobility Controller and Mobility Agent

Command	Purpose
show wireless mobility summary	Displays the summary information for the Mobility Controller and Mobility Agent.

show wireless mobility statistics	Displays mobility statistics.
show wireless mobility dtls connections	Displays established DTLS connections.

Table 95: Monitoring Mobility Configuration Commands on the Mobility Oracle

Command	Purpose
show wireless mobility oracle summary	Displays the status of the Mobility Controllers known to the Mobility Oracle.
show wireless mobility oracle client summary	Displays the information of a list of clients in the Mobility Oracle database.
show wireless mobility oracle client detail *client -mac-address*	Displays the detailed information of a particular client in the Mobility Oracle database.
show wireless mobility oracle *mc-ip*	Displays the information of a list of clients in the Mobility Oracle database that are anchored or associated to a specified Mobility Controller.

Table 96: Monitoring Mobility Configuration Commands on the Mobility Controller

Command	Purpose
show wireless mobility controller client summary	Displays a list of clients in the subdomain.
show wireless mobility controller client *mac-address* **detail**	Displays detailed information for a client in a subdomain.
show wireless mobility agent *ma-ip* **client summary**	Displays a list of clients anchored or associated to a specified Mobility Agent.
show wireless mobility ap-list	Displays the list of Cisco APs known to the mobility group.

Table 97: Monitoring Mobility Configuration Commands on the Mobility Agent

Command	Purpose
show wireless mobility load-balance summary	Displays the summary of mobility load-balance properties.

Additional References for Configuring Client Roaming

Related Documents

Related Topic	Document Title
Mobility configuration	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Related Topic	Document Title
Mobility-related commands	*Mobility Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

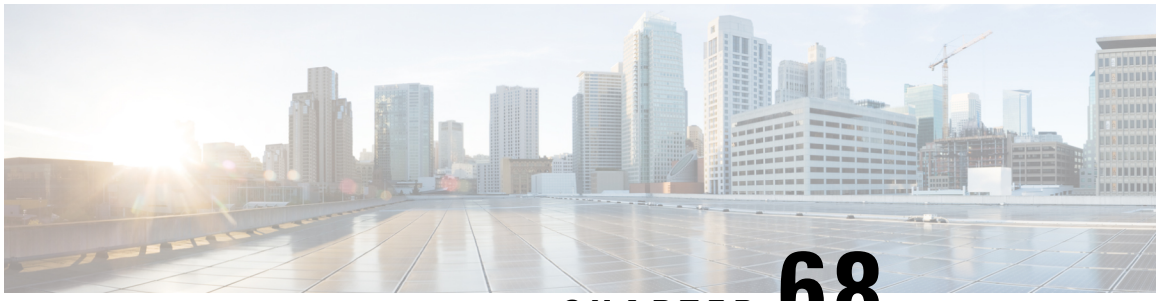
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Performing Client Roaming Configuration

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 68

Configuring Application Visibility and Control

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Application Visibility and Control

Application Visibility and Control (AVC) classifies applications using deep packet inspection techniques with the Network-Based Application Recognition engine, and provides application-level visibility and control (QoS) in wireless networks. After the applications are recognized, the AVC feature enables you to either drop, mark, or police the data traffic.

AVC is configured by defining a class map in a QoS client policy to match a protocol.

Using AVC, we can detect more than 1000 applications. AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades.

Note You can view list of 30 applications in Top Applications in Monitor Summary section of the UI.

Traffic flows are analyzed and recognized using the NBAR2 engine at the access point. For more information about the NBAR2 Protocol Library, see http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html. The specific flow is marked with the recognized protocol or application, such as WebEx. This per-flow information can be used for application visibility using Flexible NetFlow (FNF).

AVC QoS actions are applied with AVC filters in both upstream and downstream directions. The QoS actions supported for upstream flow are drop, mark, and police, and for downstream flow are mark and police. AVC QoS is applicable only when the application is classified correctly and matched with the class map filter in the policy map. For example, if the policy has a filter based on an application name, and the traffic has also been classified to the same application name, then the action specified for this match in the policy will be applied.

Note When you downgrade the controller from 8.0 to any earlier version, the AVC rate limit rules display the action as drop. This action is expected since the AVC rate limit rule is introduced in the controller version 8.0.

Cisco WLC Platform	Flow
Cisco 2504 WLC	26,250
Cisco 5508 WLC	183,750
Cisco WiSM2	393,750
Cisco 8510 WLC	336,000
Cisco 5520 WLC	336,000
Cisco 8540 WLC	336,000

Application Visibility and Control Protocol Packs

Protocol packs are a means to distribute protocol updates outside the switch software release trains, and can be loaded on the switch without replacing the switch software.

The Application Visibility and Control Protocol Pack (AVC Protocol Pack) is a single compressed file that contains multiple Protocol Description Language (PDL) files and a manifest file. A set of required protocols can be loaded, which helps AVC to recognize additional protocols for classification on your network. The manifest file gives information about the protocol pack, such as the protocol pack name, version, and some information about the available PDLs in the protocol pack.

The AVC Protocol Packs are released to specific AVC engine versions. You can load a protocol pack if the engine version on the switch platform is the same or higher than the version required by the protocol pack.

AAA override for AVC profiles

The AAA attribute for client or user profile is configured on the AAA server using authentication from RADIUS server or Cisco ACS or ISE. The AAA attribute is processed during layer 2 or layer 3 authentication by the switch and the same is overridden by what is configured on the WLAN.

The AAA AVC profile is defined as a Cisco AV air. The string option is defined as **avc-profile-name** and this value has to be configured for any AVC profile available in the switch.

Supported AVC Class Map and Policy Map Formats

Supported AVC Class Map Format

Class Map Format	Class Map Example	Direction
match protocol *protocol name*	`class-map match-any webex-class match protocol webex-media`	Both upstream and downstream
match protocol attribute category *category-name*	`class-map match-any IM match protocol attribute category instant-messaging`	Both upstream and downstream
match protocol attribute sub-category *sub-category-name*	`class-map match-any realtimeconferencing match protocol attribute sub-category voice-video-chat-collaboration`	Both upstream and downstream
match protocol attribute application-group *application-group-name*	`class-map match-any skype match protocol attribute application-group skype-group`	Both upstream and downstream
Combination filters	`class-map match-any webex-class match protocol webex match dscp 45 match wlan user-priority 6`	Upstream only

Supported AVC Policy Format

Policy Format	QoS Action
Upstream client policy based on match protocol filter	Mark, police, and drop
Downstream client policy based on match protocol filter	Mark and police

The following table describes the detailed AVC policy format with an example:

AVC Policy Format	AVC Policy Example	Direction
Basic set	`policy-map webex-policy  class webex-class  set dscp ef //or set up,cos`	Upstream and downstream

AVC Policy Format	AVC Policy Example	Direction

Basic police	`policy-map webex-policy`
	` class webex-class`
	` police 5000000`
		Upstream and downstream

Basic set and police	`policy-map webex-policy`
	` class webex-class`
	` set dscp ef //or set up,cos`
	`police 5000000`
		Upstream and downstream

Multiple set and police including default	`policy-map webex-policy`
	` class webex-class`
	` set dscp af31 //or set up,cos`
	
	` police 4000000`
	` class class-webex-category`
	` set dscp ef //or set up,cos`
	` police 6000000`
	` class class-default`
	` set dscp <>`
		Upstream and downstream

Hierarchical police	`policy-map webex-policy`
	` class webex-class`
	` police 5000000`
	` service-policy`
	`client-in-police-only`
	
	` policy-map`
	`client-in-police-only`
	` class webex-class`
	` police 100000`
	` class class-webex-category`
	` set dscp ef //or set up,cos`
	` police 6000000`
	` police 200000`
		Upstream and downstream

Hierarchical set and police	`policy-map webex-policy`
	` class class-default`
	` police 1500000`
	` service policy`
	`client-up-child`
	` policy-map webex-policy`
	` class webex-class`
	` police 100000`
	` set dscp ef`
	` class class-webex-category`
	` police 200000`
	` set dscp af31`	

AVC Policy Format	AVC Policy Example	Direction

Drop action	Any of the above examples apply to this format with this additional example:
	`policy-map webex-policy`
	` class webex-class`
	` drop`
	` class netflix`
	` set dscp ef //or set up,cos`
	` police 6000000`
	` class class-default`
	` set dscp <>`
		Upstream only

Prerequisites for Application Visibility and Control

- The access points should be AVC capable.
- For the control part of AVC (QoS) to work, the application visibility feature with FNF has to be configured.

Guidelines for Inter-Switch Roaming with Application Visibility and Control

Follow these guidelines to prevent clients from getting excluded due to malformed QoS policies:

- When a new QoS policy is added to the switch, a QoS policy with the same name should be added to other switch within the same roam or mobility domain.
- When a switch is loaded with a software image of a later release, the new policy formats are supported. If you have upgraded the software image from an earlier release to a later release, you should save the configuration separately. When an earlier release image is loaded, some QoS policies might show as not supported, and you should restore those QoS policies to supported policy formats.

Restrictions for Application Visibility and Control

- AVC is supported only on the following access points:
  - Cisco Aironet 1260 Series Access Points
  - Cisco Aironet 1600 Series Access Points
  - Cisco Aironet 2600 Series Access Point
  - Cisco Aironet 2600 Series Wireless Access Points
  - Cisco Aironet 2700 Series Access Point
  - Cisco Aironet 3500 Series Access Points

- Cisco Aironet 3600 Series Access Points

- AVC is not supported on Cisco Aironet 702W, 702I (128 M memory), and 1530 Series Access Points.
- Dropping or marking of the data traffic (control part) is not supported for software Release 3.3.
- Dropping or marking of the data traffic (control part) is supported in software Release 3E.
- Only the applications that are recognized with application visibility can be used for applying QoS control.
- Multicast traffic classification is not supported.
- Only the applications that are recognized with App visibility can be used for applying QoS control.
- IPv6 including ICMPv6 traffic classifications are not supported.
- Datalink is not supported for NetFlow fields for AVC.
- The following commands are not supported for AVC flow records:
  - **collect flow username**
  - **collect interface** { **input** | **output**}
  - **collect wireless client ipv4 address**
  - **match interface** { **input** | **output**}
  - **match transport igmp type**
- The template timeout cannot be modified on exporters configured with AVC. Even if the template timeout value is configured to a different value, only the default value of 600 seconds is used.
- For the username information in the AVC-based record templates, ensure that you configure the options **records** to get the user MAC address to username mapping.
- When there is a mix of AVC-enabled APs such as 3600, and non-AVC-enabled APs such as 1140, and the chosen policy for the client is AVC-enabled, the policy will not be sent to the APs that cannot support AVC.
- Only ingress AVC statistics are supported. The frequency of statistics updates depends on the number of clients loaded at the AP at that time. Statistics are not supported for very large policy format sizes.
- The total number of flows for which downstream AVC QoS supported per client is 1000.
- The maximum number of flows supported for Cisco WLC 5700 Series is 360 K and Catalyst 3850 Series Switch is 48 K.
- These are some class map and policy map-related restrictions. For supported policy formats, see Supported AVC Class Map and Policy Map Formats, on page 1299

  .

  - AVC and non-AVC classes cannot be defined together in a policy in a downstream direction. For example, when you have a class map with match protocol, you cannot use any other type of match filter in the policy map in the downstream direction.
  - Drop action is not applicable for the downstream AVC QoS policy.
  - Match protocol is not supported in ingress or egress for SSID policy.

- Google shares resources among several of their services because of which for some of the traffic it is not possible to say it is unique to one application. Therefore we added google-services for traffic that cannot be distinguished. The behavior you experience is expected.

How to Configure Application Visibility and Control

Configuring Application Visibility and Control (CLI)

To configure Application Visibility, follow these general steps:

1. Create a flow record by specifying keys and non-key fields to the flow.
2. Create an optional flow exporter by specifying the flow record as an option.
3. Create a flow monitor based on the flow record and flow exporter.
4. Configure WLAN to apply flow monitor in IPv4 input or output direction.

To configure Application Control, follow these general steps:

1. Create an AVC QoS policy.
2. Attach AVC QoS policy to the client in one of three ways: configuring WLAN, using ACS or ISE, or adding local policies.

Creating a Flow Record

By default, **wireless avc basic** (flow record) is available. When you click **Apply** from the GUI, then the record is mapped to the flow monitor.

Default flow record cannot be edited or deleted. If you require a new flow record, you need to create one and map it to the flow monitor from CLI.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 2	**flow record** *flow_record_name*
	Example:
	`Switch(config)# flow record record1`
	`Switch (config-flow-record)#`
		Enters flow record configuration mode.

Step 3	**description** *string* **Example:** `Switch(config-flow-record)# description IPv4flow`	(Optional) Describes the flow record as a maximum 63-character string.
Step 4	**match ipv4 protocol** **Example:**	Specifies a match to the IPv4 protocol.

	Command or Action	Purpose
	`Switch (config-flow-record)# match ipv4 protocol`	
Step 5	**match ipv4 source address** **Example:** `Switch (config-flow-record)# match ipv4 source address`	Specifies a match to the IPv4 source address-based field.
Step 6	**match ipv4 destination address** **Example:** `Switch (config-flow-record)# match ipv4 destination address`	Specifies a match to the IPv4 destination address-based field.
Step 7	**match transport source-port** **Example:** `Switch (config-flow-record)# match transport source-port`	Specifies a match to the transport layer source-port field.
Step 8	**match transport destination-port** **Example:** `Switch (config-flow-record)# match transport destination-port`	Specifies a match to the transport layer destination-port field.
Step 9	**match flow direction** **Example:** `Switch (config-flow-record)# match flow direction`	Specifies a match to the direction the flow was monitored in.
Step 10	**match application name** **Example:** `Switch (config-flow-record)# match application name`	Specifies a match to the application name. **Note** This action is mandatory for AVC support, as this allows the flow to be matched against the application.
Step 11	**match wireless ssid** **Example:** `Switch (config-flow-record)# match wireless ssid`	Specifies a match to the SSID name identifying the wireless network.
Step 12	**collect counter bytes long** **Example:** `Switch (config-flow-record)# collect counter bytes long`	Specifies to collect counter fields total bytes.
Step 13	**collect counter packets long** **Example:** `Switch (config-flow-record)# collect counter bytes long`	Specifies to collect counter fields total packets.

	Command or Action	Purpose
Step 14	**collect wireless ap mac address** **Example:** `Switch (config-flow-record)# collect wireless ap mac address`	Specifies to collect the BSSID with MAC addresses of the access points that the wireless client is associated with.
Step 15	**collect wireless client mac address** **Example:** `Switch (config-flow-record)# collect wireless client mac address`	Specifies to collect MAC address of the client on the wireless network. **Note** The **collect wireless client mac address** is mandatory configuration for wireless AVC.
Step 16	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating a Flow Exporter (Optional)

You can create a flow export to define the export parameters for a flow. This is an optional procedure for configuring flow parameters.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 2	**flow exporter** *flow_exporter_name*
	Example:
	`Switch(config)# flow exporter record1`
	`Switch (config-flow-exporter)#`
		Enters flow exporter configuration mode.

Step 3	**description** *string* **Example:** `Switch(config-flow-exporter)# description IPv4flow`	Describes the flow record as a maximum 63-character string.
Step 4	**destination** *{hostname | ip-address}* **Example:** `Switch (config-flow-exporter) # destination 10.99.1.4`	Specifies the hostname or IPv4 address of the system to which the exporter sends data.
Step 5	**transport udp** *port-value* **Example:**	Configures a port value for the UDP protocol.

	Command or Action	Purpose
	`Switch (config-flow-exporter) # transport udp 2`	
Step 6	**option application-table timeout** *seconds* **(optional)** **Example:** `Switch (config-flow-exporter)# option application-table timeout 500`	(Optional) Specifies application table timeout option. The valid range is from 1 to 86400 seconds.
Step 7	**option usermac-table timeout** *seconds* **(optional)** **Example:** `Switch (config-flow-exporter)# option usermac-table timeout 1000`	(Optional) Specifies wireless usermac-to-username table option. The valid range is from 1 to 86400 seconds.
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 9	**show flow exporter** **Example:** `Switch # show flow exporter`	Verifies your configuration.
Step 10	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating a Flow Monitor

You can create a flow monitor and associate it with a flow record and a flow exporter.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**flow monitor** *monitor-name* **Example:** `Switch (config)# flow monitor flow-monitor-1`	Creates a flow monitor and enters flow monitor configuration mode.
Step 3	**description** *description* **Example:**	Creates a description for the flow monitor.

	Command or Action	Purpose
	`Switch (config-flow-monitor)# description flow-monitor-1`	
Step 4	**record** *record-name* **Example:** `Switch (config-flow-monitor)# record flow-record-1`	Specifies the name of a recorder that was created previously.
Step 5	**exporter** *exporter-name* **Example:** `Switch (config-flow-monitor)# exporter flow-exporter-1`	Specifies the name of an exporter that was created previously.

Step 6	**cache timeout** {**active** | **inactive**} **(Optional)**
	Example:
	`Switch (config-flow-monitor)# cache timeout active 1800`
	`Switch (config-flow-monitor)# cache timeout inactive 200`
		Specifies to configure flow cache parameters. You can configure for a time period of 1 to 604800 seconds (optional).
		Note To achieve optimal result for the AVC flow monitor, we recommend you to configure the inactive cache timeout value to be greater than 90 seconds.

Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 8	**show flow monitor** **Example:** `Switch # show flow monitor`	Verifies your configuration.

Creating AVC QoS Policy

To create AVC QoS policy, perform these general steps:

1. Create a class map with match protocol filters.
2. Create a policy map.
3. Apply a policy map to the client in one of the following ways:
   1. Apply a policy map over WLAN either from the CLI or GUI.
   2. Apply a policy map through the AAA server (ACS server or ISE) from the CLI.

      For more information, refer to the *Cisco Identity Services Engine User Guide* and *Cisco Secure Access Control System User Guide*.
   3. Apply local policies either from the CLI or GUI.

Creating a Class Map

You need to create a class map before configuring any match protocol filter. The QoS actions such as marking, policing, and dropping can be applied to the traffic. The AVC match protocol filters are applied only for the wireless clients. For more information about the protocols that are supported, see http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**class-map** *class-map-name* **Example:** `Switch(config)# class-map webex-class`	Creates a class map.

Step 3	**match protocol** {*application-name* | **attribute category** *category-name* | **attribute sub-category** *sub-category-name* | **attribute application-group** *application-group-name*}
	Example:
	`Switch(config)# class-map webex-class`
	`Switch(config-cmap)# match protocol webex-media`
	
	`Switch(config)# class-map class-webex-category`
	`Switch(config-cmap)# match protocol attribute category webex-media`
	
	`Switch# class-map class-webex-sub-category`
	`Switch(config-cmap)# match protocol attribute sub-category webex-media`
	
	`Switch# class-map class-webex-application-group`
	`Switch(config-cmap)# match protocol attribute application-group webex-media`
		Specifies match to the application name, category name, subcategory name, or application group.

Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating a Policy Map

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 2	**policy-map** *policy-map-name*
	Example:
	`Switch(config)# policy-map webex-policy`
	`Switch(config-pmap)#`
		Creates a policy map by entering the policy map name, and enters policy-map configuration mode.
		By default, no policy maps are defined.
		The default behavior of a policy map is to set the DSCP to 0 if the packet is an IP packet and to set the CoS to 0 if the packet is tagged. No policing is performed.
		Note To delete an existing policy map, use the **no policy-map** *policy-map-name* global configuration command.

Step 3	**class** [*class-map-name* | **class-default**]
	Example:
	`Switch(config-pmap)# class-map webex-class`
	`Switch(config-pmap-c)#`
		Defines a traffic classification, and enters policy-map class configuration mode.
		By default, no policy map and class maps are defined.
		If a traffic class has already been defined by using the **class-map** global configuration command, specify its name for *class-map-name* in this command.
		A **class-default** traffic class is predefined and can be added to any policy. It is always placed at the end of a policy map. With an implied **match any** is included in the **class-default** class, all packets that have not already matched the other traffic classes will match **class-default**.
		Note To delete an existing class map, use the **no class** *class-map-name* policy-map configuration command.

Step 4	**police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}] **Example:** `Switch(config-pmap-c)# police 100000 80000 drop`	Defines a policer for the classified traffic. By default, no policer is defined. • For *rate-bps,* specify an average traffic rate in bits per second (b/s). The range is 8000 to 10000000000.

	Command or Action	Purpose
		• For *burst-byte,* specify the normal burst size in bytes. The range is 8000 to 1000000. • (Optional) Specifies the action to take when the rates are exceeded. Use the **exceed-action drop** keywords to drop the packet. Use the **exceed-action policed-dscp-transmit** keywords to mark down the DSCP value (by using the policed-DSCP map) and to send the packet.
Step 5	**set** {**dscp** *new-dscp* | **cos** *cos-value*} **Example:** `Switch(config-pmap-c)# set dscp 45`	Classifies IP traffic by setting a new value in the packet. • For **dscp** *new-dscp*, enter a new DSCP value to be assigned to the classified traffic. The range is 0 to 63.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

What to do next

After creating your policy maps, attach the traffic policy or polices to an interface using the **service-policy** command.

Configuring Local Policies (CLI)

Configuring Local Policies (CLI)

To configure local policies, complete these procedures:

1. Create a service template.
2. Create an interface template.
3. Create a parameter map.
4. Create a policy map.
5. Apply a local policy on a WLAN.

Creating a Service Template (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Switch# configure terminal`	

Step 2	**service-template** *service-template-name*
	Example:
	`Switch(config)# service-template cisco-phone-template`
	`Switch(config-service-template)#`
		Enters service template configuration mode.

Step 3	**access-group** *acl_list* **Example:** `Switch(config-service-template)# access-group foo-acl`	Specifies the access list to be applied.
Step 4	**vlan** *vlan_id* **Example:** `Switch(config-service-template)# vlan 100`	Specifies VLAN ID. You can specify a value from 1 to 4094.
Step 5	**absolute-timer** *seconds* **Example:** `Switch(config-service-template)# absolute-timer 20`	Specifies session timeout value for service template. You can specify a value from 1 to 65535.
Step 6	**service-policy qos** {**input** | **output**} **Example:** `Switch(config-service-template)# service-policy qos input foo-qos`	Configures QoS policies for the client.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating a Parameter Map (CLI)

Parameter map is preferred to use than class map.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**parameter-map type subscriber attribute-to-service** *parameter-map-name* **Example:** `Switch(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para`	Specifies the parameter map type and name.
Step 3	*map-index* **map** { **device-type** | **mac-address** | **oui** | **user-role** | **username**} {**eq** | **not-eq** | **regex** *filter-name* } **Example:** `Switch(config-parameter-map-filter)# 10 map device-type eq "WindowsXP-Workstation"`	Specifies parameter map attribute filter criteria.

Step 4	**service-template** *service-template-name*
	Example:
	`Switch(config-parameter-map-filter-submode)# service-template cisco-phone-template`
	`Switch(config-parameter-map-filter-submode)#`
		Enters service template configuration mode.

Step 5	**interface-template** *interface-template-name*
	Example:
	`Switch(config-parameter-map-filter-submode)# interface-template cisco-phone-template`
	`Switch(config-parameter-map-filter-submode)#`
		Enters service template configuration mode.

Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Information About Configuring Local Policies, on page 486
Restrictions for Configuring Local Policies, on page 485
Monitoring Local Policies, on page 496
Examples: Local Policies Configuration, on page 497

Creating a Policy Map (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**policy-map type control subscriber** *policy-map-name* **Example:** `Switch(config)# policy-map type control subscriber Aironet-Policy`	Specifies the policy map type.
Step 3	**event identity-update** {**match-all** | **match-first**} **Example:** `Switch(config-policy-map)# event identity-update match-all`	Specifies match criteria to the policy map.
Step 4	*class_number* **class** {*class_map_name* | **always** } {**do-all** | **do-until-failure** | **do-until-success**} **Example:** `Switch(config-class-control-policymap)# 1 class local_policy1_class do-until-success`	Configures the local profiling policy class map number and specifies how to perform the action. The class map configuration mode includes the following command options: • **always**—Executes without doing any matching but return success. • **do-all**—Executes all the actions. • **do-until-failure**—Execute all the actions until any match failure is encountered. This is the default value. • **do-until-success**—Execute all the actions until any match success happens.
Step 5	*action-index* **map attribute-to-service table** *parameter-map-name* **Example:** `Switch(config-policy-map)# 10 map attribute-to-service table Aironet-Policy-para`	Specifies parameter map table to be used.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Information About Configuring Local Policies, on page 486
Restrictions for Configuring Local Policies, on page 485
Monitoring Local Policies, on page 496
Examples: Local Policies Configuration, on page 497

Applying a Local Policy for a Device on a WLAN (CLI)

Before you begin

If the service policy contains any device type-based rules in the parameter map, ensure that the device classifier is already enabled.

Note You should use the **device classification** command to classify the device for it to be displayed correctly on the show command output.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name* **Example:** `Switch(config)# wlan wlan1`	Enters WLAN configuration mode.
Step 3	**service-policy type control subscriber** *policymapname* **Example:** `Switch(config-wlan)# service-policy type control subscriber Aironet-Policy`	Applies local policy to WLAN.
Step 4	**profiling local http (optional)** **Example:** `Switch(config-wlan)# profiling local http`	Enables only profiling of devices based on HTTP protocol (optional).
Step 5	**profiling radius http (optional)** **Example:** `Switch(config-wlan)# profiling radius http`	Enables profiling of devices on ISE (optional).
Step 6	**no shutdown** **Example:**	Specifies not to shut down the WLAN.

	Command or Action	Purpose
	`Switch(config-wlan)# no shutdown`	
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Information About Configuring Local Policies, on page 486
Restrictions for Configuring Local Policies, on page 485
Monitoring Local Policies, on page 496
Examples: Local Policies Configuration, on page 497

Configuring Local Policies (GUI)

Configuring Local Policies (GUI)

To configure local policies, complete these procedures:

Procedure

	Command or Action	Purpose
Step 1	Create a service template.	
Step 2	Create a policy map.	
Step 3	Apply a local policy that you have created to a WLAN.	

Creating a Service Template (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Local Policies** > **Service Template** to open the **Service Template** page.

Step 2 Create a new template as follows:

a) Click **New** to open the **Service Template > New** page.
b) In the Service Template name text box, enter the new service template name.
c) In the VLAN ID text box, enter the VLAN identifier that has to be associated with the policy. The value ranges from 1 to 4094.
d) In the Session timeout text box, enter the maximum amount of time, in seconds, after which a client is forced to reauthenticate. The value ranges from 1 to 65535 seconds.
e) From the Access control list drop-down list, choose the access control list to be mapped to the policy.
f) From the Ingress QoS drop-down list, choose the ingress QoS policy to be applied.
g) From the Egress QoS drop-down list, choose the egress QoS policy to be applied.
h) Click **Apply** to save the configuration.

Step 3 Edit a service template as follows:

a) From the **Service Template** page, click the service template to open the **Service Template > Edit** page.

b) In the VLAN ID text box, enter the VLAN identifier that has to be associated with the policy. The value ranges from 1 to 4094.
c) In the Session timeout text box, enter the maximum amount of time, in seconds, after which a client is forced to reauthenticate. The value ranges from 1 to 65535 seconds.
d) From the Access control list drop-down list, choose the access control list to be mapped to the policy.
e) From the Ingress QoS drop-down list, choose the ingress QoS policy to be applied.
f) From the Egress QoS drop-down list, choose the egress QoS policy to be applied.
g) Click **Apply** to save the configuration.

Step 4 Remove a service template as follows:

a) From the **Service Template** page, select the service template.
b) Click **Remove**.
c) Click **Apply** to save the configuration.

Related Topics

Information About Configuring Local Policies, on page 486
Restrictions for Configuring Local Policies, on page 485
Monitoring Local Policies, on page 496
Examples: Local Policies Configuration, on page 497

Creating a Policy Map (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Local Policies** > **Policy Map** to open the **Policy Map** page.

Step 2 Create a new policy map as follows:

a) Click **New** to open the **Policy Map > New** page.
b) In the Policy Map name text box, enter the new policy map name.
c) Click **Add** to open the Match Criteria area.
d) From the Device Type drop-down list, choose the device type. The match criteria for the device type can be eq, not-eq, or regex with respect to the device type you are choosing.
e) From the User Role drop-down list, select the match criteria as eq, not-eq, or regex and enter the user type or user group of the user, for example, student, teacher, and so on.
f) From the Service Template drop-down list, choose the service template to be mapped to the policy.
g) Click **Add**. The match criteria is added to the Match Criteria Lists.
h) In the Match Criteria Lists area, click **Add** to add the match criteria to the policy.
i) Click **Apply** to save the configuration.

Step 3 Edit a policy map as follows:

a) In the **Policy Map** page, select the policy map that you want to edit, and click **Edit** to open the **Policy Map > Edit** page.
b) In the Match Criteria area, choose the device type from the Device Type drop-down list. The match criteria for the device type can be eq, not-eq, or regex with respect to the device type you are choosing.
c) In the Match Criteria area, choose the user role from the User Role drop-down list. Select the match criteria as eq, not-eq, or regex and enter the user type or user group of the user
d) From the Service Template drop-down list, choose the service template to be mapped to the policy.

e) Click **Ok** to save the configuration or **Cancel** to discard the configuration.
f) Click **Add** to add more match criteria based on device type, user role, and service template to the policy.
g) In the Match Criteria Lists area, select the match criteria and click **Move to** to move the match criteria with respect to a value entered in the row text box.
h) Select the match criteria and click **Move up** to move the match criteria up in the list.
i) Select the match criteria and click **Move down** to move the match criteria down in the list.
j) Select the match criteria and click **Remove** to remove the match criteria from the policy map list.
k) Click **Apply** to save the configuration.

Step 4 Remove a policy map as follows:

a) From the **Policy Map** page, select the policy map.
b) Click **Remove**.
c) Click **Apply** to save the configuration.

Related Topics

Information About Configuring Local Policies, on page 486
Restrictions for Configuring Local Policies, on page 485
Monitoring Local Policies, on page 496
Examples: Local Policies Configuration, on page 497

Applying Local Policies to WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **WLAN** to open the **WLANs** page.
Step 2 Click the corresponding WLAN profile. The **WLANs > Edit** page is displayed.
Step 3 Click the **Policy-Mapping** tab.
Step 4 Check the **Device Classification** check box to enable classification based on device type.
Step 5 From the Local Subscriber Policy drop-down list, choose the policy that has to be applied for the WLAN.
Step 6 Select **Local HTTP Profiling** to enable profiling on devices based on HTTP (optional).
Step 7 Select **Radius HTTP Profiling** to enable profiling on devices based on RADIUS (optional).
Step 8 Click **Apply** to save the configuration.

Related Topics

Information About Configuring Local Policies, on page 486
Restrictions for Configuring Local Policies, on page 485
Monitoring Local Policies, on page 496
Examples: Local Policies Configuration, on page 497

Configuring WLAN to Apply Flow Monitor in IPV4 Input/Output Direction

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-id* **Example:** `Switch (config) # wlan 1`	Enters WLAN configuration submode. For *wlan-id*, enter the WLAN ID. The range is 1 to 64.
Step 3	**ip flow monitor** *monitor-name* **{input | output}** **Example:** `Switch (config-wlan) # ip flow monitor flow-monitor-1 input`	Associates a flow monitor to the WLAN for input or output packets.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Application Visibility and Control (GUI)

Configuring Application Visibility (GUI)

You can apply the default flow record (**wireless avc basic**) to the default flow monitor (**wireless-avc-basic**).

If you are using the flow record and flow monitor you have created, then the record name and monitor name should be same. This is specific only for configuring AVC from GUI and not for the CLI configuration.

You can use the flow monitor you have created either for upstream or downstream, or both, but ensure that you use the same record name while mapping with the flow monitor.

Procedure

Step 1 Choose **Configuration** > **Wireless** > **WLAN**.

The **WLAN** page appears.

Step 2 Click on the corresponding WLAN ID to open the **WLAN > Edit** page and click **AVC**.

The **Application Visibility** page appears.

a) Select the **Application Visibility Enabled** check box to enable AVC on a WLAN.
b) In the **Upstream Profile** text box, enter the name of the AVC profile.
c) In the **Downstream Profile** text box, enter the name of the AVC profile.

To enable AVC, you need to enter the profile names for the upstream and downstream profiles. The profile names are the flow monitor names. By default, the flow monitor names (**wireless-avc-basic**) appear in the **Upstream Profile** and **Downstream Profile** text boxes. For the default flow monitor, the default flow record (**wireless avc basic**) will be taken. The default flow record is generated by the system and is available.

You can change the profile names for the upstream and downstream profiles but ensure that the same flow records are available for the flow monitors.

The upstream and downstream profiles can have different profile names but there should be flow records available for the flow monitors.

Step 3 Click **Apply** to apply AVC on the WLAN.

Step 4 To disable AVC on a specific WLAN, perform the following steps:

- Choose **Configuration** > **Wireless** > **WLAN** to open the **WLAN** page.
- Click on the corresponding WLAN ID to open the **WLAN > Edit** page.
- Click **AVC** to open the **Application Visibility** page.
- Uncheck the **Application Visibility Enabled** check box.
- Click **Apply** to disable AVC on the specific WLAN.

Configuring Application Visibility and Control (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless**.

Step 2 Expand the **QoS** node by clicking the left pane and choosing **QOS-Policy**.

The **QOS-Policy** page is displayed.

Step 3 Click **Add New** to create a new QoS Policy.

The **Create QoS Policy** page is displayed.

Step 4 Select **Client** from the Policy Type drop-down list.

Step 5 Select the direction into which the policy needs to be applied from the Policy Direction drop-down list.

The available options are:

- **Ingress**
- **Egress**

Step 6 In the **Policy Name** text box, specify a policy name.

Step 7 In the **Description** text box, provide a description to the policy.

Step 8 Check the **Enable Application Recognition** check box to configure the AVC class map for a client policy.

Note For an egress client policy, when you enable Application Recognition, the Voice, Video, and User Defined check boxes are disabled.

The following options are available:

- **Trust**—Specify a classification type for this policy.
  - **Protocol**—Allows you to choose the protocols and configure the marking and policing of the packets.
  - **Category**—Allows you to choose the category of the application, for example, browsing.
  - **Subcategory**—Allows you to choose the subcategory of the application, for example, file-sharing.
  - **Application-Group**—Allows you to choose the application group, for example, ftp-group.
- **Protocol Choice**—Choose the protocols, category, subcategory, or application group from the **Available Protocols** list into the **Assigned Protocols** to apply the marking and policing of the packets.
- **Mark**—Specify the marking label for each packet. The following options are available:
  - **DSCP**—Assigns a label to indicate the given quality of service. The range is from 0 to 63.
  - **CoS**—Matches IEEE 802.1Q class of service. The range is from 0 to 7.
  - **None**—Does not mark the packets.
- **Police (kbps)**—Specify the policing rate in kbps. This option is available when the **Policy Direction** is egress.
- **Drop**—Specify to drop the ingress packets that correspond to the chosen protocols.

Note You can add a maximum of five AVC classes for each client policy.

Step 9 Click **Add** to create an AVC class map. The new class map is listed in a tabular format.

Step 10 Click **Apply** to create an AVC QoS policy.

Step 11 Click the QoS policy link in the **QOS-Policy** page to edit the QoS policy. The **QOS-Policy** > **Edit** page is displayed. Make changes and click **Apply** to commit your changes.

Step 12 Remove an AVC class map from the QoS policy by navigating to the corresponding AVC class map row in the AVC class map table and clicking **Remove**. Click **Apply** to commit your changes.

Monitoring Application Visibility and Control

Monitoring Application Visibility and Control (CLI)

This section describes the new commands for application visibility.

The following commands can be used to monitor application visibility on the switch and access points.

Table 98: Monitoring Application Visibility Commands on the switch

Command	Purpose
show avc client *client-mac* **top** *n* **application** [**aggregate** | **upstream** | **downstream**]	Displays information about top "N" applications for the given client MAC.
show avc wlan *ssid* **top** *n* **application** [**aggregate** | **upstream** | **downstream**]	Displays information about top "N" applications for the given SSID.
avc top user[enable | disable]	Enables or disables the information about top "N" application.

show avc wlan *wlan-id* **application** *app name* **top***N* [**aggregate** | **upstream** | **downstream**]	Displays to know network usage information on a per user basis within an application. **Note** On Catalyst 4500E Supervisor Engine 8-E, in the information about top N users that is displayed, the client's MAC address and username are not displayed. This issue occurs only within 90 seconds after the client is disconnected.
show wlan id *wlan-id*	Displays information whether AVC is enabled or disabled on a particular WLAN.
show flow monitor *flow_monitor_name* **cache**	Displays information about flow monitors.
show wireless client mac-address *mac-address* **service-policy** { **input** | **output** }	Displays information about policy mapped to the wireless clients.

Table 99: Clearing Application Visibility Statistics Commands

Command	Purpose
clear avc client *mac* **stats**	Clears the statistics per client.
clear avc wlan *wlan-name* **stats**	Clears the statistics per WLAN.

Monitoring Application Visibility and Control (GUI)

You can view AVC information on a WLAN in a single shot using a **AVC on WLAN** pie chart on the **Home** page of the switch. The pie chart displays the AVC data (Aggregate - Application Cumulative usage %) of the first WLAN. In addition, the top 5 WLANs based on clients are displayed first. Click on any one of the WLANs to view the corresponding pie chart information. If AVC is not enabled on the first WLAN, then the **Home** page does not display the AVC pie chart.

Procedure

Step 1 Choose **Monitor** > **Controller** > **AVC** > **WLANs**.

The **WLANs** page appears.

Step 2 Click the corresponding WLAN profile.

The **Application Statistics** page appears.

From the **Top Applications** drop-down list, choose the number of top applications you want to view and click **Apply**. The valid range is between 5 to 30, in multiples of 5.

a) On the Aggregate, Upstream, and Downstream tabs, you can view the application cumulative and last 90 seconds statistics and usage percent with the following fields:

- Application name
- Packet count

- Byte count
- Average packet size
- usage (%)

Step 3 Choose **Monitor** > **Clients** > **Client Details** > **Clients**.

The **Clients** page appears.

Step 4 Click **Client MAC Address** and then click **AVC Statistics** tab.

The **Application Visibility** page appears.

a) On the Aggregate, Upstream, and Downstream tabs, you can view the application cumulative and last 90 seconds statistics and usage percent with the following fields:

- Application name
- Packet count
- Byte count
- Average packet size
- usage (%)

Monitoring SSID and Client Policies Statistics (GUI)

Statistics are supported only for ingress policies with a maximum of five classes on wireless targets. For very large policies, statistics for ingress policies are not visible at the switch. The frequency of the statistics depends on the number of clients associated with the access point.

Type of Statistics	Method	Details
SSID Policies	Choose **Monitor > Controller > Statistics > QoS**.	The QoS page is displayed with a list of SSID policies, Radio Type, and AP. Choose an SSID policy, radio, and access point from the drop-down lists and click **Apply** to view the statistics of the chosen SSID policy. You can view details such as match criteria, confirmed bytes, conformed rate, and exceeded rate.

Type of Statistics	Method	Details
Client Policies	Choose **Monitor > Clients > Client Details** .	The Clients page is displayed with a list of client MAC addresses, AP, and other details. Click the MAC address of a client and click the **QoS Statistics** tab. You can view details such as match criteria, confirmed bytes, conformed rate, and exceeded rate.

Examples: Application Visibility and Control

Examples: Application Visibility Configuration

This example shows how to create a flow record, create a flow monitor, apply the flow record to the flow monitor, and apply the flow monitor on a WLAN:

```
Switch# configure terminal
Switch(config)# flow record fr_v4
Switch(config-flow-record)# match ipv4 protocol
Switch(config-flow-record)# match ipv4 source address
Switch(config-flow-record)# match ipv4 destination address
Switch(config-flow-record)# match transport destination-port
Switch(config-flow-record)# match flow direction
Switch(config-flow-record)# match application name
Switch(config-flow-record)# match wireless ssid
Switch(config-flow-record)# collect counter bytes long
Switch(config-flow-record)# collect counter packets long
Switch(config-flow-record)# collect wireless ap mac address
Switch(config-flow-record)# collect wireless client mac address
Switch(config)#end
```

```
Switch# configure terminal
Switch# flow monitor fm_v4
Switch(config-flow-monitor)# record fr_v4
Switch(config-flow-monitor)# cache timeout active 1800
Switch(config)#end
```

```
Switch(config)#wlan wlan1
Switch(config-wlan)#ip flow monitor fm_v4 input
Switch(config-wlan)#ip flow mon fm-v4 output
Switch(config)#end
```

Examples: Application Visibility and Control QoS Configuration

This example shows how to create class maps with apply match protocol filters for application name, category, and subcategory:

```
Switch# configure terminal
Switch(config)# class-map cat-browsing
Switch(config-cmap)# match protocol attribute category browsing
Switch(config-cmap)#end

Switch# configure terminal
Switch(config)# class-map cat-fileshare
Switch(config-cmap)# match protocol attribute category file-sharing
Switch(config-cmap)#end

Switch# configure terminal
Switch(config)# class-map match-any subcat-terminal
Switch(config-cmap)# match protocol attribute sub-category terminal
Switch(config-cmap)#end

Switch# configure terminal
Switch(config)# class-map match-any webex-meeting
Switch(config-cmap)# match protocol webex-meeting
Switch(config-cmap)#end
```

This example shows how to create policy maps and define existing class maps for upstream QoS:

```
Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class cat-browsing
Switch(config-pmap-c)# police 150000
Switch(config-pmap-c)# set dscp 12
Switch(config-pmap-c)#end


Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class cat-fileshare
Switch(config-pmap-c)# police 1000000
Switch(config-pmap-c)# set dscp 20
Switch(config-pmap-c)#end


Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class subcat-terminal
Switch(config-pmap-c)# police 120000
Switch(config-pmap-c)# set dscp 15
Switch(config-pmap-c)#end

Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class webex-meeting
Switch(config-pmap-c)# police 50000000
Switch(config-pmap-c)# set dscp 21
Switch(config-pmap-c)#end
```

This example shows how to create policy maps and define existing class maps for downstream QoS:

```
Switch# configure terminal
Switch(config)# policy-map test-avc-down
Switch(config-pmap)# class cat-browsing
Switch(config-pmap-c)# police 200000
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)#end
```

```
Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class cat-fileshare
Switch(config-pmap-c)# police 300000
Switch(config-pmap-c)# set wlan user-priority 2
Switch(config-pmap-c)# set dscp 20
Switch(config-pmap-c)#end
```

```
Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class subcat-terminal
Switch(config-pmap-c)# police 100000
Switch(config-pmap-c)# set dscp 25
Switch(config-pmap-c)#end
```

```
Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class webex-meeting
Switch(config-pmap-c)# police 60000000
Switch(config-pmap-c)# set dscp 41
Switch(config-pmap-c)#end
```

This example shows how to apply defined QoS policy on a WLAN:

```
Switch# configure terminal
Switch(config)#wlan  alpha
Switch(config-wlan)#shut
Switch(config-wlan)#end
Switch(config-wlan)#service-policy client input test-avc-up
Switch(config-wlan)#service-policy client output test-avc-down
Switch(config-wlan)#no shut
Switch(config-wlan)#end
```

Example: Configuring QoS Attribute for Local Profiling Policy

The following example shows how to configure QoS attribute for a local profiling policy:

```
Switch(config)# class-map type control subscriber match-all local_policy1_class
Switch(config-filter-control-classmap)# match device-type android
Switch(config)# service-template local_policy1_template
Switch(config-service-template)# vlan 40
Switch(config-service-template)# service-policy qos output local_policy1
Switch(config)# policy-map type control subscriber local_policy1
Switch(config-event-control-policymap)# event identity-update match-all
Switch(config-class-control-policymap)# 1 class local_policy1_class do-until-success
Switch(config-action-control-policymap)# 1 activate service-template local_policy1_template
Switch(config)# wlan open_auth 9
Switch(config-wlan)# client vlan VLAN40
Switch(config-wlan)# service-policy type control subscriber local_policy1
```

Additional References for Application Visibility and Control

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
Flexible NetFlow configuration	*Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
Flexible NetFlow commands	*Flexible NetFlow Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
QoS configuration	*QoS Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)*
QoS commands	*QoS Command Reference, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

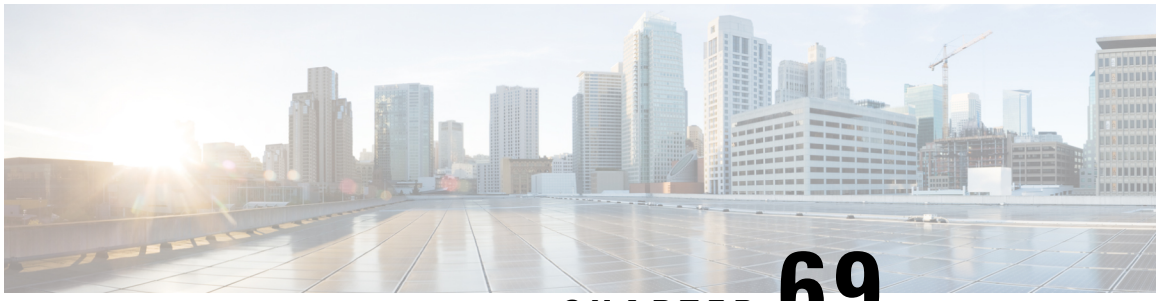
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Application Visibility and Control

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.
Cisco IOS XE 3E	AVC control with QoS was introduced.



CHAPTER 69

Configuring Voice and Video Parameters

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Voice and Video Parameters

You can confirm the following points before configuring voice and video parameters:

- Ensure that the switch has access points connected to it.
- Configure SSID.

Restrictions for Voice and Video Parameters

The following are the restrictions that you should keep in mind while configuring voice and video parameters:

- SIP CAC can be used for the 9971 Cisco phones that support TSPEC-based admission control. You can also use the phones that support Status code 17.

- SIP snooping is supported for providing voice priority to the non-TSPEC SIP phones.
- TSPEC for video CAC is not supported.
- The following features are not supported for the 802.11ac module on the Cisco 3600 Access Point:
  - Voice support
  - CAC support
  - TSM support
- When the 802.11ac module is enabled, the 11n LBCAC parameters can be inaccurate resulting in degradation in voice quality of 11ac enabled calls.
- Cisco 792x IP phones that are admitted as non-WMM devices with 11K enabled will experience audio problems with the phones.

Note Disable 11K for voice WLAN for all 792x Cisco IP phones that are admitted as non-WMM devices with 11K enabled. Upgrade the firmware on Cisco Unified Call Manager to 1.4.5 to resolve this issue. Refer to the Cisco Unified Call Manager configuration guide for more information.

Information About Configuring Voice and Video Parameters

Three parameters on the switch affect voice and/or video quality:

- Call Admission Control
- Expedited bandwidth requests
- Unscheduled automatic power save delivery

Call Admission Control (CAC) and UAPSD are supported on Cisco Compatible Extensions (CCX) v4 and v5; however, these parameters are also supported even without CCX but on any device implementing WMM (that supports 802.1e). Expedited bandwidth requests are supported only on CCXv5.

Traffic stream metrics (TSM) can be used to monitor and report issues with voice quality.

Call Admission Control

Call Admission Control (CAC) enables an access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion. The WMM protocol deployed in CCXv4 maintains QoS under differing network loads.

Two types of Over The Air (OTA) CAC are available: static-based CAC and load-based CAC.

The switch supports the following QoS policies:

- User-defined policies: You can define your own QoS policies. You can have more control over these policies than the existing metal policies.

- System-defined precious metal policies: To support backward compatibility.
  - Platinum: Used for VoIP clients.
  - Gold: Used for video clients.
  - Silver: Used for best effort traffic.
  - Bronze: Used for NRT traffic.

Static-Based CAC

Voice over WLAN applications supporting WMM and TSPEC can specify how much bandwidth or shared medium time is required to initiate a call. Bandwidth-based, or static, CAC enables the access point to determine whether it is capable of accommodating a particular call. The access point rejects the call if necessary in order to maintain the maximum allowed number of calls with acceptable quality.

The QoS setting for a WLAN determines the level of bandwidth-based CAC support. To use bandwidth-based CAC with voice applications, the WLAN must be configured for Platinum QoS. With bandwidth-based CAC, the access point bandwidth availability is determined based on the amount of bandwidth currently used by the access point clients, to which the bandwidth requested by the Voice over WLAN applications is added. If this total exceeds a configured bandwidth threshold, the new call is rejected.

Note You must enable admission control (ACM) for CCXv4 clients that have WMM enabled. Otherwise, bandwidth-based CAC does not operate properly for these CCXv4 clients.

Load-Based CAC

Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types (including that from clients), cochannel access point loads, and coallocated channel interference, for voice and video applications. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

In load-based CAC, the access point continuously measures and updates the utilization of the RF channel (that is, the mean time of bandwidth that has been exhausted), channel interference, and the additional calls that the access point can admit. The access point admits a new call only if the channel has enough unused bandwidth to support that call. By doing so, load-based CAC prevents oversubscription of the channel and maintains QoS under all conditions of WLAN loading and interference.

Note If you disable load-based CAC, the access points start using bandwidth-based CAC.

IOSd Call Admission Control

IOSd Call Admission Control (CAC) controls bandwidth availability from switch to access point.

You can configure class-based, unconditional packet marking features on your switch for CAC.

CAC is a concept that applies to voice and video traffic only—not data traffic. If an influx of data traffic oversubscribes a particular link in the network, queueing, buffering, and packet drop decisions resolve the

congestion. The extra traffic is simply delayed until the interface becomes available to send the traffic, or, if traffic is dropped, the protocol or the end user initiates a timeout and requests a retransmission of the information.

Network congestion cannot be resolved in this manner when real-time traffic, sensitive to both latency and packet loss, is present, without jeopardizing the quality of service (QoS) expected by the users of that traffic. For real-time delay-sensitive traffic such as voice, it is better to deny network access under congestion conditions than to allow traffic onto the network to be dropped and delayed, causing intermittent impaired QoS and resulting in customer dissatisfaction.

CAC is therefore a deterministic and informed decision that is made before a voice call is established and is based on whether the required network resources are available to provide suitable QoS for the new call.

Based on the admit CAC CLI configuration in addition to the existing CAC algorithm, switch allows either voice or video with TSPEC or SIP snooping. The **admit cac** CLI is mandatory for the voice call to pass through.

If the BSSID policer is configured for the voice or video traffic, then additional checks are performed on the packets.

Expedited Bandwidth Requests

The expedited bandwidth request feature enables CCXv5 clients to indicate the urgency of a WMM traffic specifications (TSPEC) request (for example, an e911 call) to the WLAN. When the controller receives this request, it attempts to facilitate the urgency of the call in any way possible without potentially altering the quality of other TSPEC calls that are in progress.

You can apply expedited bandwidth requests to both bandwidth-based and load-based CAC. Expedited bandwidth requests are disabled by default. When this feature is disabled, the controller ignores all expedited requests and processes TSPEC requests as normal TSPEC requests.

The following table lists examples of TSPEC request handling for normal TSPEC requests and expedited bandwidth requests.

Table 100: TSPEC Request Handling Examples

CAC Mode	Reserved bandwidth for voice calls	Usage	Normal TSPEC Request	TSPEC with Expedited Bandwidth Request
Bandwidth-based CAC	75% (default setting)	Less than 75%	Admitted	Admitted
		Between 75% and 90% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 90%	Rejected	Rejected
Load-based CAC		Less than 75%	Admitted	Admitted
		Between 75% and 85% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 85%	Rejected	Rejected

[17] For bandwidth-based CAC, the voice call bandwidth usage is per access point radio and does not take into account cochannel access points. For load-based CAC, the voice call bandwidth usage is measured for the entire channel.

[18] Bandwidth-based CAC (consumed voice and video bandwidth) or load-based CAC (channel utilization [Pb]).

Note Admission control for TSPEC G711-20ms and G711-40 ms codec types are supported.

U-APSD

Unscheduled automatic power save delivery (U-APSD) is a QoS facility defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending battery life, this feature reduces the latency of traffic flow delivered over the wireless media. Because U-APSD does not require the client to poll each individual packet buffered at the access point, it allows delivery of multiple downlink packets by sending a single uplink trigger packet. U-APSD is enabled automatically when WMM is enabled.

Traffic Stream Metrics

In a voice-over-wireless LAN (VoWLAN) deployment, traffic stream metrics (TSM) can be used to monitor voice-related metrics on the client-access point air interface. It reports both packet latency and packet loss. You can isolate poor voice quality issues by studying these reports.

The metrics consist of a collection of uplink (client side) and downlink (access point side) statistics between an access point and a client device that supports CCX v4 or later releases. If the client is not CCX v4 or CCXv5 compliant, only downlink statistics are captured. The client and access point measure these metrics. The access point also collects the measurements every 5 seconds, prepares 90-second reports, and then sends the reports

to the controller. The controller organizes the uplink measurements on a client basis and the downlink measurements on an access point basis and maintains an hour's worth of historical data. To store this data, the controller requires 32 MB of additional memory for uplink metrics and 4.8 MB for downlink metrics.

TSM can be configured through either the GUI or the CLI on a per radio-band basis (for example, all 802.11a radios). The controller saves the configuration in flash memory so that it persists across reboots. After an access point receives the configuration from the controller, it enables TSM on the specified radio band.

This table shows the upper limit for TSM entries in different controller series.

TSM Entries	5700
MAX AP TSM entries	100
MAX Client TSM entries	250
MAX TSM entries	100*250=25000

Note Once the upper limit is reached, additional TSM entries cannot be stored and sent to WCS or NCS. If client TSM entries are full and AP TSM entries are available, then only the AP entries are stored, and viceversa. This leads to partial output. TSM cleanup occurs every one hour. Entries are removed only for those APs and clients that are not in the system.

Information About Configuring Voice Prioritization Using Preferred Call Numbers

You can configure a switch to provide support for SIP calls from VoWLAN clients that do not support TSPEC-based calls. This feature is known as SIP CAC support. If bandwidth is available in the configured voice pool, the SIP call uses the normal flow and the switch allocates the bandwidth to those calls.

You can also prioritize up to six preferred call numbers. When a call comes to one of the configured preferred numbers, the switch does not check the configured maximum voice bandwidth. The switch allocates the bandwidth needed for the call, even if it exceeds the maximum bandwidth for voice configured for voice CAC. The preferred call will be rejected if bandwidth allocation exceeds 85% of the radio bandwidth. The bandwidth allocation is 85 percent of the entire bandwidth pool, not just from the maximum configured voice pool. The bandwidth allocation is the same even for roaming calls.

You must configure the following parameters before configuring voice prioritization:

- Set WLAN QoS to allow voice calls to pass through.
- Enable ACM for the radio.
- Enable SIP call snooping on the WLAN.

Information About EDCA Parameters

Enhanced distributed channel access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality-of-service (QoS) traffic.

How to Configure Voice and Video Parameters

Configuring Voice Parameters (CLI)

Before you begin

Ensure that you have configured SIP-based CAC.

You should have created a class map for CAC before beginning this procedure.

Procedure

	Command or Action	Purpose
Step 1	**show wlan summary** **Example:** `Switch# show wlan summary`	Specifies all of the WLANs configured on the switch.
Step 2	**show wlan** *wlan_id* **Example:** `Switch# show wlan 25`	Specifies the WLAN that you plan to modify. For voice over WLAN, ensure that the WLAN is configured for WMM and the QoS level is set to Platinum.
Step 3	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 4	**policy-map** *policy-map name*
	Example:
	`Switch(config)# policy-map test_2000`
	`Switch(config-pmap)#`
		Enters policy map configuration mode.
		Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
		In WLAN, you need to configure service-policy for these commands to take effect.

Step 5	**class** {*class-name* | **class-default**}
	Example:
	`Switch(config-pmap)# class test_1000`
	`Switch(config-pmap-c)#`
		Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change.
		Specifies the name of the class whose policy you want to create or change.
		You can also create a system default class for unclassified packets.

Step 6	**admit cac wmm-tspec** **Example:**	(Optional) Admits the request for Call Admission Control (CAC) for policy map.

	Command or Action	Purpose
	`Switch(config-pmap-c)# admit cac wmm-tspec` `Switch(config-pmap-c)#`	

Step 7	**service-policy** *policy-map name*
	Example:
	`Switch(config-pmap-c)# service-policy test_2000`
	`Switch(config-pmap-c)#`
		Configures the QoS service policy.

Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Step 9	**wlan** *wlan_profile_name wlan_ID SSID_network_name* **wlan shutdown**
	Example:
	`Switch(config)# wlan wlan1`
	`Switch(config-wlan)# wlan shutdown`
		Disables all WLANs with WMM enabled prior to changing the video parameters.

Step 10	**wlan** *wlan_profile_name wlan_ID SSID_network_name*
	Example:
	`Switch(config)# wlan wlan1`
	`Switch(config-wlan)# wlan shutdown`
		Disables all WLANs with WMM enabled prior to changing the voice parameters.

Step 11	**wlan** *wlan_name* **call-snoop** **Example:** `Switch(config)# wlan wlan1 call-snoop`	Enables the call-snooping on a particular WLAN.

Step 12	**wlan** *wlan_name* **service-policy input** *input_policy_name*
	Example:
	`Switch(config)# wlan wlan1`
	`Switch(config-wlan)# service-policy input platinum-up`
		Configures input SSID policy on a particular WLAN to voice.

Step 13	**wlan** *wlan_name* **service-policy output** *ouput_policy_name*
	Example:
	`Switch(config)# wlan wlan1`
	`Switch(config-wlan)# service-policy output platinum`
		Configures output SSID policy on a particular WLAN to voice.

Step 14	**wlan** *wlan_name* **service-policy input** *ingress_policy_name*	Configures ingress SSID policy on a particular WLAN as user-defined policy.

	Command or Action	Purpose

	Example:
	`Switch(config)# wlan wlan1`
	`Switch(config-wlan)# service-policy input policy1`	

Step 15	**wlan** *wlan_name* **service-policy output** *egress_policy_name*
	Example:
	`Switch(config)# wlan wlan1`
	`Switch(config-wlan)# service-policy output policy2`
		Configures egress SSID policy on a particular WLAN as user-defined policy.

Step 16	**ap dot11 {5ghz | 24ghz} shutdown** **Example:**	Disables the radio network. `Switch(config)# ap dot11 5ghz shutdown`
Step 17	**ap dot11 {5ghz | 24ghz} cac voice sip** **Example:** `Switch(config)# ap dot11 5ghz cac voice sip`	Enables or disables SIP IOSd CAC for the 802.11a or 802.11b/g network.
Step 18	**ap dot11 {5ghz | 24ghz} cac voice acm** **Example:** `Switch(config)# ap dot11 5ghz cac voice acm`	Enables or disables bandwidth-based voice CAC for the 802.11a or 802.11b/g network.
Step 19	**ap dot11 {5ghz | 24ghz} cac voice max-bandwidth** *bandwidth* **Example:** `Switch(config)# ap dot11 5ghz cac voice max-bandwidth 85`	Sets the percentage of maximum bandwidth allocated to clients for voice applications on the 802.11a or 802.11b/g network. The bandwidth range is 5 to 85%, and the default value is 75%. Once the client reaches the value specified, the access point rejects new videos on this network.
Step 20	**ap dot11 {5ghz | 24ghz} cac voice roam-bandwidth** *bandwidth* **Example:** `Switch(config)# ap dot11 5ghz cac voice roam-bandwidth 10`	Sets the percentage of maximum allocated bandwidth reserved for roaming voice clients. The bandwidth range is 0 to 25%, and the default value is 6%. The switch reserves this much bandwidth from the maximum allocated bandwidth for roaming voice clients.
Step 21	**no wlan shutdown** **Example:** `Switch(config-wlan)# no wlan shutdown`	Reenables all WLANs with WMM enabled.
Step 22	**no ap dot11 {5ghz | 24ghz} shutdown** **Example:**	Reenables the radio network.

	Command or Action	Purpose
	`Switch(config)# no ap dot11 5ghz shutdown`	
Step 23	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Example

Configuring Video Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**show wlan summary** **Example:** `Switch# show wlan summary`	Specifies all of the WLANs configured on the switch.
Step 2	**show wlan** *wlan_id* **Example:** `Switch# show wlan 25`	Specifies the WLAN that you plan to modify.
Step 3	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 4	**policy-map** *policy-map name*
	Example:
	`Switch(config)# policy-map test_2000`
	`Switch(config-pmap)#`
		Enters policy map configuration mode.
		Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
		In WLAN, you need to configure service-policy for these commands to take effect.

Step 5	**class** {*class-name* | **class-default**}
	Example:
	`Switch(config-pmap)# class test_1000`
	`Switch(config-pmap-c)#`
		Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change.
		Specifies the name of the class whose policy you want to create or change.
		You can also create a system default class for unclassified packets.

	Command or Action	Purpose

Step 6	**admit cac wmm-tspec**
	Example:
	`Switch(config-pmap-c)# admit cac wmm-tspec`
	`Switch(config-pmap-c)#`
		(Optional) Admits the request for Call Admission Control (CAC) for policy map.

Step 7	**service-policy** *policy-map name*
	Example:
	`Switch(config-pmap-c)# service-policy test_2000`
	`Switch(config-pmap-c)#`
		Configures the QoS service policy.

Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Step 9	**wlan***wlan_profile_name*
	Example:
	`Switch(config)# wlan wlan1`
	`Switch(config-wlan)# wlan shutdown`
		Disables all WLANs with WMM enabled prior to changing the video parameters.

Step 10	**ap dot11 {5ghz | 24ghz} shutdown** **Example:** `Switch(config)# ap dot11 5ghz shutdown`	Disables the radio network.
Step 11	**ap dot11 {5ghz | 24ghz} cac video acm** **Example:** `Switch(config)# ap dot11 5ghz cac video acm`	Enables or disables bandwidth-based video CAC for the 802.11a or 802.11b/g network.
Step 12	**ap dot11 {5ghz | 24ghz} cac video load-based** **Example:** `Switch(config)# ap dot11 5ghz cac video load-based`	Configures the load-based CAC method. If you do not enter this command, then the default static CAC is applied.
Step 13	**ap dot11 {5ghz | 24ghz} cac video max-bandwidth** *bandwidth* **Example:** `Switch(config)# ap dot11 5ghz cac video max-bandwidth 20`	Sets the percentage of maximum bandwidth allocated to clients for video applications on the 802.11a or 802.11b/g network. The bandwidth range is 5 to 85%, and the default value is 75%. The default value is 0, which means no bandwidth request control. The sum of the voice bandwidth and video bandwidth should not exceed 85% or configured maximum media bandwidth.

	Command or Action	Purpose
Step 14	**ap dot11 {5ghz | 24ghz} cac video roam-bandwidth** *bandwidth* **Example:** `Switch(config)# ap dot11 5ghz cac video roam-bandwidth 9`	Sets the percentage of maximum allocated bandwidth reserved for roaming clients for video. The bandwidth range is 0 to 25%, and the default value is 0%.
Step 15	**no wlan shutdown** *wlan_id* **Example:** `Switch(config-wlan)# no wlan shutdown 25`	Reenables all WLANs with WMM enabled.
Step 16	**no ap dot11 {5ghz | 24ghz} shutdown** **Example:** `Switch(config)# no ap dot11 5ghz shutdown`	Reenables the radio network.
Step 17	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Example

Configuring SIP-Based CAC (CLI)

SIP CAC controls the total number of SIP calls that can be made.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 2	**wlan** *wlan-name*
	Example:
	`Switch(config)# wlan qos-wlan`
	`Switch(config-wlan)#`
		Enters WLAN configuration submode.

Step 3	**call-snoop** **Example:** `Switch(config-wlan)# call-snoop`	Enables the call-snooping feature for a particular WLAN.

	Command or Action	Purpose
Step 4	**service-policy** [**client**] **input** *policy-map name* **Example:** `Switch(config-wlan)# service-policy input platinum-up`	Assigns a policy map to WLAN input traffic. Ensure that you provide QoS policy to voice for input traffic.
Step 5	**service-policy** [**client**] **output** *policy-map name* **Example:** `Switch(config-wlan)# service-policy output platinum`	Assigns policy map to WLAN output traffic. Ensure that you provide QoS policy to voice for output traffic.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 7	**show wlan** {*wlan-id* | *wlan-name*} **Example:** `Switch# show wlan qos-wlan`	Verifies the configured QoS policy on the WLAN.
Step 8	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 9	**ap dot11 {5ghz | 24ghz} cac {voice | video} acm** **Example:** `Switch(config)# ap dot11 5ghz cac voice acm`	Enables the ACM static on the radio. When enabling SIP snooping, use the static CAC, not the load-based CAC.
Step 10	**ap dot11 {5ghz | 24ghz} cac voice sip** **Example:** `Switch(config)# ap dot11 5ghz cac voice sip`	Configures SIP-based CAC.
Step 11	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Example

Configuring a Preferred Call Number (CLI)

Before you begin

You must set the following parameters before configuring a preferred call number.

- Set WLAN QoS to voice.
- Enable ACM for the radio.
- Enable SIP call snooping on the WLAN.
- Enable SIP-based CAC.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 2	**wlan** *wlan-name* **qos platinum**
	Example:
	`Switch(config)# wlan wlan1`
	`Switch(config-wlan)# qos platinum`
		Sets QoS to voice on a particular WLAN.

Step 3	**ap dot11 {5ghz | 24ghz} cac {voice | video} acm** **Example:** `Switch(config)# ap dot11 5ghz cac voice acm`	Enables the static ACM on the radio. When enabling SIP snooping, use the static CAC, not the load-based CAC.

Step 4	**wlan** *wlan-name*
	Example:
	`Switch(config)# wlan wlan1`
	`Switch(config-wlan)# call-snoop`
		Enables the call-snooping feature for a particular WLAN.

Step 5	**wireless sip preferred-call-no** *call_index call_number* **Example:** `Switch(config)# wireless sip preferred-call-no 1 555333`	Adds a new preferred call.
Step 6	**no wireless sip preferred-call-no** *call_index*	Removes a preferred call.

	Command or Action	Purpose
	Example: `Switch(config)# no wireless sip preferred-call-no 1`	
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Example

Configuring EDCA Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 {5ghz | 24ghz } shutdown** **Example:** `Switch(config)# ap dot11 5ghz shutdown`	Disables the radio network.
Step 3	**ap dot11 {5ghz | 24ghz} edca-parameters {custom-voice | fastlane | optimized-video-voice | optimized-voice | svp-voice | wmm-default}** **Example:** `Switch(config)# ap dot11 5ghz edca-parameters optimized-voice`	Enables a specific EDCA parameters for the 802.11a or 802.11b/g network. • custom-voice—Enables custom voice parameters for the 802.11a or 802.11b/g network. • fastlane—Enables fastlane parameters for the 802.11a or 802.11b/g network. • optimized-video-voice—Enables EDCA voice- and video-optimized parameters for the 802.11a or 802.11b/g network. Choose this option when both voice and video services are deployed on your network. • optimized-voice—Enables non-SpectraLink voice-optimized profile parameters for the 802.11a or 802.11b/g network. Choose this option when voice services other than SpectraLink are deployed on your network.

	Command or Action	Purpose
		• svp-voice—Enables SpectraLink voice priority parameters for the 802.11a or 802.11b/g network. Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls. • wmm-default—Enables the Wi-Fi Multimedia (WMM) default parameters for the 802.11a or 802.11b/g network. This is the default option. Choose this option when voice or video services are not deployed on your network.
Step 4	**no ap dot11 {5ghz | 24ghz} shutdown** **Example:** `Switch(config)# no ap dot11 5ghz shutdown`	Re-enables the radio network.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show ap dot11 {5ghz | 24ghz} network** **Example:** `Switch# show ap dot11 5ghz network`	Displays the current status of MAC optimization for voice.

Configuring EDCA Parameters (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **802.11a/n/ac** > **EDCA Parameters** or **Configuration** > **Wireless** > **802.11b/g/n** > **EDCA Parameters** to open EDCA Parameters page.

Step 2 Choose one of the following options from the **EDCA Profile** drop-down list:

- **wmm-default**—Enables the Wi-Fi Multimedia (WMM) default parameters. This is the default value. Choose this option when voice or video services are not deployed on your network.
- **svp-voice**—Enables SpectraLink voice priority parameters. Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls.
- **optimized-voice**—Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than SpectraLink are deployed on your network.
- **optimized-video-voice**—Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.
- **custom-voice**—Enables custom voice EDCA parameters for 802.11a. The EDCA parameters under this option also match the 6.0 WMM EDCA parameters when this profile is applied.

Note If you deploy video services, admission control (ACM) must be disabled.

Step 3 If you want to enable MAC optimization for voice, select the **Enable Low Latency MAC** check box. Otherwise, leave this check box unselected, which is the default value. This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight access points, which improves the number of voice calls serviced per access point.

Note We do not recommend you to enable low latency MAC. You should enable low latency MAC only if the WLAN allows WMM clients. If WMM is enabled, then low latency MAC can be used with any of the EDCA profiles.

Step 4 Click **Apply** to commit your changes.

Step 5 To reenable the radio network, choose **Network** under 802.11a/n/ac or 802.11b/g/n, select the **802.11a/n/ac** (or **802.11b/g/n**) **Network Status** check box, and click **Apply**.

Step 6 Click **Save Configuration**.

Monitoring Voice and Video Parameters

This section describes the new commands for the voice and video parameters.

The following commands can be used to monitor voice and video parameters.

Table 101: Monitoring Voice Parameters Commands

Command	Purpose
show ap dot11 {5ghz | 24ghz} network	Displays the radio-based statistics for voice.
show ap name *ap_name* **dot11 24ghz tsm all**	Displays the TSM voice metrics and current status of MAC optimization for voice.
show ap name *apname* **cac voice**	Displays the information about CAC for a particular access point.
show client detail *client_mac*	Displays the U-APSD status for a particular client.
show policy-map interface wireless client	Displays the video client policy details.
show access-list	Displays the video client dynamic access-list from the switch.
show wireless client voice diag status	Displays information about whether voice diagnostics are enabled or disabled. If enabled, this also displays information about the clients in the watch list and the time remaining for the diagnostics of the voice call. **Note** To work on voice diagnostics CLIs, you need to enter the following command: **debug voice-diagnostic mac-addr** *client_mac_01 client_mac_02*

show wireless client voice diag tspec	Displays the TSPEC information sent from the clients that are enabled for voice diagnostics.
show wireless client voice diag qos-map	Displays information about the QoS/DSCP mapping and packet statistics in each of the four queues: VO, VI, BE, BK. The different DSCP values are also displayed.
show wireless client voice diag rssi	Display the client's RSSI values in the last 5 seconds when voice diagnostics is enabled.
show client voice-diag roam-history	Displays information about the last three roaming calls. The output contains the timestamp, access point associated with roaming, roaming reason, and if there is a roaming failure, reason for roaming-failure.
show policy-map interface wireless mac *mac-address*	Displays information about the voice and video data packet statistics.
show wireless media-stream client summary	Displays a summary of the media stream and video client information.
show controllers d0 | b queue	Displays which queue the packets are going through on an access point.
show platform qos queue stats *interface*	Displays which queue packets are going through from the switch.

You can monitor the video parameters using the following commands.

Table 102: Monitoring Video Parameters Commands

Command	Purpose
show ap join stats summary *ap_mac*	Displays the last join error detail for a specific access point.
show ip igmp snooping wireless mgid	Displays the TSM voice metrics and current status of MAC optimization for voice.
show wireless media-stream multicast-direct state	Displays the media stream multicast-direct parameters.
show wireless media-stream group summary	Displays the summary of the media stream and client information.
show wireless media-stream group detail *group_name*	Displays the details of a specific media-stream group.
show wireless media-stream client summary	Displays the details for a set of media-stream clients.
show wireless media-stream client detail *group_name*	Displays the details for a set of media-stream clients.
show ap dot11 {5ghz | 24ghz) media-stream rrc	Display the details of media stream.
show wireless media-stream message details	Displays information about the message configuration.

show ap name *ap-name* **auto-rf dot11 5ghz | i Util**	Displays the details of channel utilization.
show controllers d0 | b queue	Displays which queue the packets are going through on an access point based on 2.4- and 5-GHz bands.
show controllers d1 | b queue	Displays which queue the packets are going through on an access point based on 2.4- and 5-GHz bands.
show cont d1 | b Media	Displays the video metric details on the band A or B.
show capwap mcast mgid all	Displays information about all of the multicast groups and their corresponding multicast group identifications (MGIDs) associated to the access point.
show capwap mcast mgid id *id*	Displays information about all of the video clients joined to the multicast group in a specific MGID.

Configuration Examples for Voice and Video Parameters

Example: Configuring Voice and Video

Configuring Egress SSID Policy for Voice and Video

The following example shows how to create and configure an egress SSID policy for voice and video:

```
table-map egress_ssid_tb
 map from 24 to 24
 map from 34 to 34
 map from 46 to 46
 default copy

class-map match-any voice
  match  dscp ef
class-map match-any video
  match  dscp af41

policy-map ssid-cac
class class-default
    shape average 25000000
   set dscp dscp table egress_ssid_tb
   queue-buffers ratio 0
   service-policy ssid-child-cac

policy-map ssid-child-cac
 class voice
    priority level 1
    police 5000000
     conform-action transmit
     exceed-action drop
    admit cac wmm-tspec
      rate 1000
      wlan-up  6 7
 class video
    priority level 2
```

```
    police 10000000
      conform-action transmit
      exceed-action drop
    admit cac wmm-tspec
      rate 3000
      wlan-up  4 5
```

Configuring Ingress SSID Policy for Voice and Video

The following example shows how to create and configure an ingress SSID policy for voice and video:

```
table-map up_to_dscp
 map from 0 to 0
 map from 1 to 8
 map from 2 to 8
 map from 3 to 0
 map from 4 to 34
 map from 5 to 34
 map from 6 to 46
 map from 7 to 48
 default copy

policy-map ingress_ssid
 class class-default
   set dscp wlan user-priority table up_to_dscp
```

Configuring Egress Port Policy Voice and Video

The following example shows how to create and configure an egress port policy for voice and video:

```
policy-map port_child_policy
 class non-client-nrt-class
 bandwidth remaining ratio 10

 class voice
 priority level 1
 police rate 3000000

 class video
 priority level 2
 police rate 4000000
```

Applying Ingress and Egress SSID policies for Voice and Video on a WLAN

The following example shows how to apply ingress and egress SSID policies for voice and video on a WLAN:

```
wlan voice_video 1 voice_video
 service-policy input ingress_ssid
 service-policy output ssid-cac
```

Additional References for Voice and Video Parameters

Related Documents

Related Topic	Document Title
Multicast configuration	*Multicast Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
VideoStream configuration	*VideoStream Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

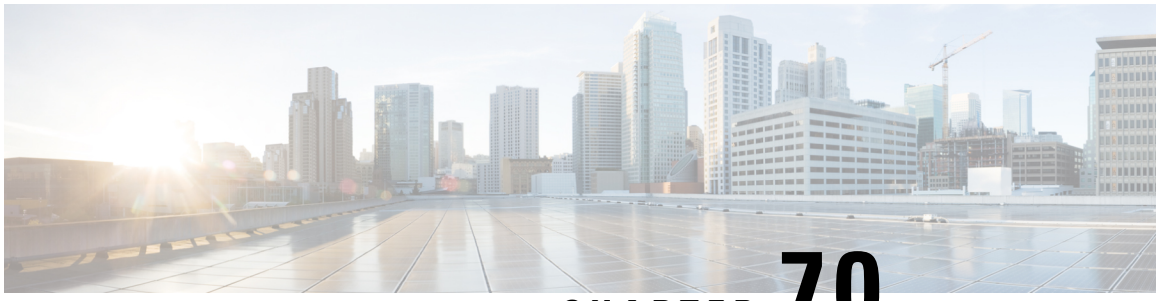
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Performing Voice and Video Parameters Configuration

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 70

Configuring RFID Tag Tracking

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configuring RFID Tag Tracking

The device enables you to configure radio-frequency identification (RFID) tag tracking. RFID tags are small wireless devices that are affixed to assets for real-time location tracking. They operate by advertising their location using special 802.11 packets, which are processed by access points, the controller, and the location appliance.

How to Configure RFID Tag Tracking

Configuring RFID Tag Tracking (CLI)

Procedure

	Command or Action	Purpose
Step 1	**location rfid status**	Enables RFID tag tracking.

	Command or Action	Purpose
	Example: `Switch(config)# location rfid status`	By default, RFID tag tracking is enabled.
Step 2	(Optional) **no location rfid status** **Example:** `Switch(config)# no location rfid status`	Disables RFID tag tracking.
Step 3	**location rfid timeout** *seconds* **Example:** `Switch(config)# location rfid timeout 1500`	Specifies a static timeout value (between 60 and 7200 seconds). The static timeout value is the amount of time that the switch maintains tags before expiring them. For example, if a tag is configured to beacon every 30 seconds, we recommend that you set the timeout value to 90 seconds (approximately three times the beacon value). The default value is 1200 seconds.
Step 4	**location rfid mobility vendor-name** *name* **Example:** `Switch(config)# location rfid mobility vendor-name Aerosct`	Enables RFID tag mobility for specific tags. When you enter the **location rfid mobility vendor-name** command, tags are unable to obtain a DHCP address for client mode when attempting to select and/or download a configuration. **Note** These commands can be used only for Pango tags. Therefore, the only valid entry for **vendor_name** is "pango" in all lowercase letters.
Step 5	(Optional) **no location rfid mobility** *name* **Example:** `Switch(config)# no location rfid mobility test`	Disables RFID tag mobility for specific tags. When you enter the **no location rfid mobility** command , tags can obtain a DHCP address. If a tag roams from one subnet to another, it obtains a new address rather than retaining the anchor state.

Monitoring RFID Tag Tracking Information

This section describes the new commands for the RFID tag tracking Information.

The following commands can be used to monitor the RFID tag tracking Information on the switch.

Table 103: Monitoring RFID Tag Tracking Information Commands

Command	Purpose
show location rfid config	Displays the current configuration for RFID tag tracking.

show location rfid detail *mac_address*	Displays the detailed information for a specific RFID tag.
show location rfid summary	Displays a list of all RFID tags currently connected to the switch.
show location rfid client	Displays a list of RFID tags that are associated to the switch as clients.

Additional References RFID Tag Tracking

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

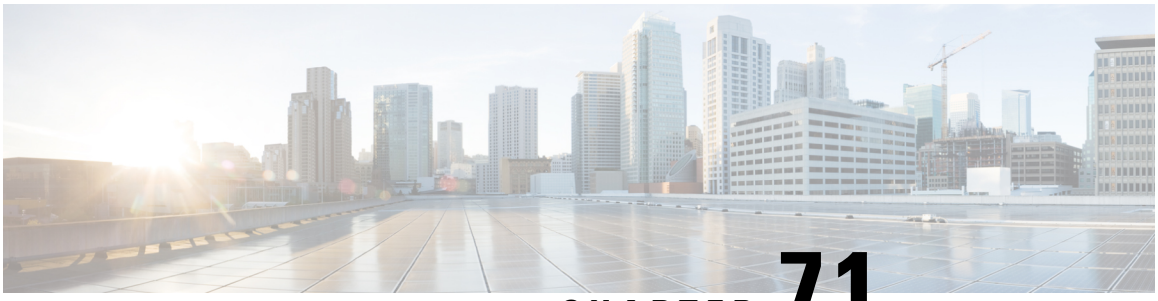
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Performing RFID Tag Tracking Configuration

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 71

Configuring Location Settings

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configuring Location Settings

The switch determines the location of client devices by gathering Received Signal Strength Indication (RSSI) measurements from access points all around the client of interest. The switch can obtain location reports from up to 16 access points for clients, RFID tags, and rogue access points.

You can configure the path loss measurement (S60) request for normal clients or calibrating clients to improve location accuracy.

How to Configure Location Settings

Configuring Location Settings (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**location plm** {**calibrating** [**multiband** | **uniband**] | **client** *burst_interval* **Example:** `Switch(config)# location plm client 100`	Configures the path loss measurement (S60) request for calibrating clients or non-calibrating. The path loss measurement request improves the location accuracy. You can configure the **burst_interval** parameter for the normal, noncalibrating client from zero through 3600 seconds, and the default value is 60 seconds. You can configure the path loss measurement request for calibrating clients on the associated 802.11a or 802.11b/g radio or on the associated 802.11a/b/g radio. If a client does not send probes often or sends them only on a few channels, its location cannot be updated or cannot be updated accurately. The **location plm** command forces clients to send more packets on all channels. When a CCXv4 (or higher) client associates, the Switch sends it a path loss measurement request, which instructs the client to transmit on the bands and channels that the access points are on (typically, channels 1, 6, and 11 for 2.4-GHz-only access points) at a configurable interval (such as 60 seconds) indefinitely.
Step 3	**location rssi-half-life** {**calibrating-client** | **client** | **rogue-aps** | **tags** } *seconds* **Example:** `Switch(config)# location rssi-half-life calibrating-client 60`	Configures the RSSI half life for the clients, calibrating clients, RFID tags, and rogue access points. You can enter the **location rssi-half-life** parameter value for the clients, calibrating clients, RFID tags, and rogue access points as 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.

	Command or Action	Purpose
		Some client devices transmit at reduced power immediately after changing channels, and RF is variable, so RSSI values might vary considerably from packet to packet. The **location rssi-half-life** command increases accuracy by averaging nonuniformly arriving data using a configurable forget period (or half life). **Note** We recommend that you do not use or modify the **location rssi-half-life** command.
Step 4	**location expiry** {**calibrating-client** | **client** | **rogue-aps** | **tags** } *timeout* **Example:** `Switch(config)# location expiry calibrating-client 50`	Configures the RSSI timeout value for the clients, calibrating clients, RFID tags, and rogue access points. You can enter the RSSI timeout value for the clients, RFID tags, and rogue access points from 5 through 3600 seconds, and the default value is 5 seconds. For the calibrating clients, you can enter the RSSI timeout value from 0 through 3600 seconds, and the default value is 5 seconds. Ensuring that recent, strong RSSIs are retained by the CPU is critical to location accuracy. The **location expiry** command enables you to specify the length of time after which old RSSI averages expire. **Note** We recommend that you do not use or modify the **location expiry** command.
Step 5	**location algorithm** {**rssi-average** | **simple**} **Example:** `Switch(config)# location algorithm rssi-average`	Configures the algorithm used to average RSSI and signal-to-noise ratio (SNR) values. You can enter the **location algorithm rssi-average** command to specify a more accurate algorithm but requires more CPU overhead or the **location algorithm simple** command to specify a faster algorithm that requires low CPU overhead but provides less accuracy. **Note** We recommend that you do not use or modify the **location algorithm** command.

	Command or Action	Purpose
Step 6	**location admin-tag** *string* **Example:** `Switch(config)# location admin-tag`	Sets administrative tag or site information for the location of client devices.
Step 7	**location civic-location identifier** {*identifier* | **host**} **Example:** `Switch(config)# location civic-location identifier host`	Specifies civic location information. You can set the civic location identifier either as a string or host.
Step 8	**location custom-location identifier** {*identifier* | **host**} **Example:** `Switch(config)# location custom-location identifier host`	Specifies custom location information. You can set the custom location identifier either as a string or host.
Step 9	**location geo-location identifier** {*identifier* | **host**} **Example:** `Switch(config)# location geo-location identifier host`	Specifies geographical location information of the client devices. You can set the location identifier either as a string or host.
Step 10	**location prefer** {**cdp** | **lldp-med** | **static**} **weight** *priority_value* **Example:** `Switch(config)# location prefer weight cdp 50`	Sets location information source priority. You can enter the priority weight from zero through 255.
Step 11	**location rfid** {**status** | **timeout** | **vendor-name**} **Example:** `Switch(config)# location rfid timeout 100`	Configures RFID tag tracking options such as RFID tag status, RFID timeout value, and RFID tag vendor name. You can enter the RFID timeout value in a range from 60 and 7200 seconds.
Step 12	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Example

Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues (CLI)

The Network Mobility Services Protocol (NMSP) manages communication between the mobility services engine and the controller for incoming and outgoing traffic. If your application requires more frequent location updates, you can modify the NMSP notification interval (to a value between 1 and 180 seconds) for clients, active RFID tags, and rogue access points and clients.

Note The TCP port (16113) that the controller and mobility services engine communicate over must be open (not blocked) on any firewall that exists between the controller and the mobility services engine for NMSP to function.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**nmsp notification interval** {**attachment** *seconds* | **location** *seconds* | **rssi** [**clients** *interval* | **rfid** *interval* | **rogues** [**ap** | **client**] *interval*]} **Example:** `Switch(config)# nmsp notification interval rssi rfid 50`	Sets the NMSP notification interval value for clients, RFID tags, and rogue clients and access points. You can enter the NMSP notification interval value for RSSI measurement from 1 through 180 seconds.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Modifying the NMSP Notification Threshold for Clients, RFID Tags, and Rogues (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**location notify-threshold** {**clients** | **rogues ap** | **tags** } *threshold* **Example:** `Switch(config)# location notify-threshold clients 5`	Configures the NMSP notification threshold for clients, RFID tags, and rogue clients and access points. You can enter the RSSI threshold value from zero through 10 db.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Monitoring Location Settings and NMSP Settings

Monitoring Location Settings (CLI)

This section describes the new commands for location settings.

The following commands can be used to monitor location settings on the switch.

Table 104: Monitoring Location Settings Commands

Command	Purpose
show location summary	Displays the current location configuration values.
show location statistics rfid	Displays the location-based RFID statistics.
show location detail *client_mac_addr*	Displays the RSSI table for a particular client.

Monitoring NMSP Settings (CLI)

The following commands can be used to monitor NMSP settings on the switch.

Table 105: Monitoring NMSP Settings Commands

Command	Purpose
show nmsp attachment suppress interfaces	Displays the attachment suppress interfaces.
show nmsp capability	Displays the NMSP capabilities.
show nmsp notification interval	Displays the NMSP notification intervals.
show nmsp statistics connection	Displays the connection-specific NMSP counters.
show nmsp statistics summary	Displays the common NMSP counters.
show nmsp status	Displays the status of active NMSP connections.
show nmsp subscription detail	Displays all of the mobility services to which the switch is subscribed.
show nmsp subscription detail *ip_addr*	Displays details only for the mobility services subscribed to by a specific IP address.
show nmsp subscription summary	Displays details for all of the mobility services to which the switch is subscribed.

Examples: Location Settings Configuration

This example shows how to configure the path loss measurement (S60) request for calibrating client on the associated 802.11a or 802.11b/g radio:

```
Switch# configure terminal
Switch(config)# location plm calibrating uniband
Switch(config)# end
Switch# show location summary
```

This example shows how to configure the RSSI half life for a rouge access point:

```
Switch# configure terminal
Switch(config)# location rssi-half-life rogue-aps 20
Switch(config)# end
Switch# show location summary
```

Examples: NMSP Settings Configuration

This example shows how to configure the NMSP notification interval for RFID tags:

```
Switch# configure terminal
Switch(config)# nmsp notification interval rssi rfid 50
Switch(config)# end
Switch# show nmsp notification interval
```

This example shows how to configure the NMSP notification interval for clients:

```
Switch# configure terminal
Switch(config)# nmsp notification interval rssi clients 180
Switch(config)# end
Switch# show nmsp notification interval
```

Additional References for Location Settings

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

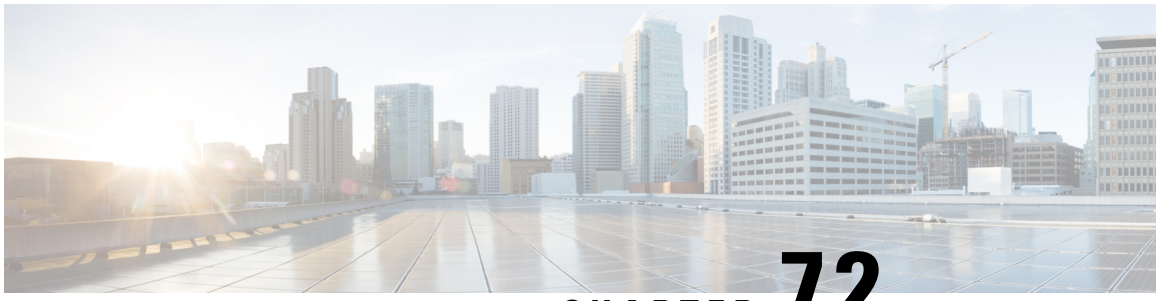
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Performing Location Settings Configuration

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 72

Monitoring Flow Control

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Flow Control

Flow control is enabled by default on the switch.

Flow control provides shim layers between WCM and Cisco IOS for a reliable IPC. Every component in WCM has a dedicated channel. Few of the components in WCM have leveraged flow control in that. There is no configuration of flow control from CLI. You can monitor the flow control for any channel.

Monitoring Flow Control

This section describes the new commands for flow control.

The following commands can be used to monitor flow control on the switch.

Table 106: Monitoring Flow Control

Command	Purpose

show wireless flow-control *channel -id*	Displays information about flow control on a particular channel.
show wireless flow-control *channel-id* **statistics**	Displays statistical information about flow control on a particular channel.

Examples: Monitoring Flow Control

This example shows how to view information pertaining to any channel:

```
Switch# show wireless flow-control 3
Switch#

Channel Name        : CAPWAP
FC State            : Disabled
Remote Server State : Enabled
Pass-thru Mode      : Disabled
EnQ Disabled        : Disabled
Queue Depth         : 2048
Max Retries         : 5
Min Retry Gap (mSec): 3
```

This example shows how to view flow control for a particular channel:

```
Switch# show wireless flow-control 3
Switch#

Channel Name                              : CAPWAP
# of times channel went into FC           : 0
# of times channel came out of FC         : 0
Total msg count received by the FC Infra  : 1
Pass-thru msgs send count                 : 0
Pass-thru msgs fail count                 : 0
# of msgs successfully queued              : 0
# of msgs for which queuing failed         : 0
# of msgs sent thru after queuing          : 0
# of msgs sent w/o queuing                 : 1
# of msgs for which send failed            : 0
# of invalid EAGAINS received              : 0
Highest watermark reached                 : 0
# of times Q hit max capacity              : 0
Avg time channel stays in FC (mSec)       : 0
```

Additional References for Monitoring Flow Control

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

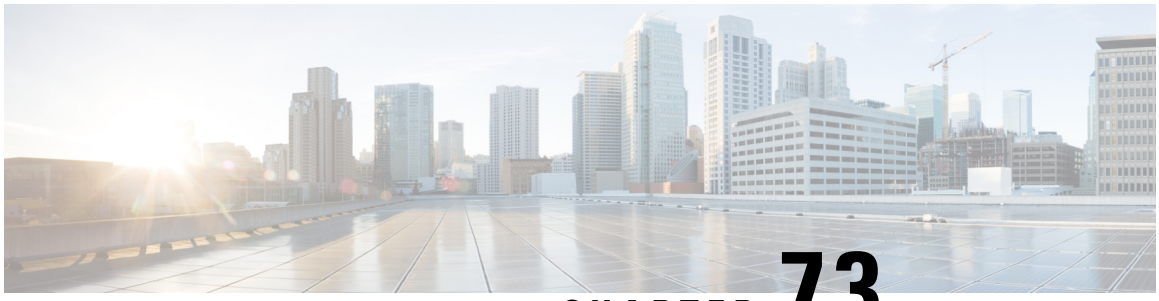
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Monitoring Flow Control

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.



CHAPTER 73

Configuring System Message Logs

Restrictions for Configuring System Message Logs

When the **logging discriminator** command is configured, the device may experience memory leak or crash. This usually happens during heavy syslog or debug output. The rate of the memory leak is dependent on the number of logs being produced. In extreme cases, the device may also crash. As a workaround, use the **no logging discriminator** command to disable the logging discriminator.

Information About Configuring System Message Logs

System Messsage Logging

By default, a switch sends the output from system messages and **debug** privileged EXEC commands to a logging process. . The logging process controls the distribution of logging messages to various destinations, such as the logging buffer, terminal lines, or a UNIX syslog server, depending on your configuration. The process also sends messages to the console.

When the logging process is disabled, messages are sent only to the console. The messages are sent as they are generated, so message and debug output are interspersed with prompts or output from other commands. Messages appear on the active consoles after the process that generated them has finished.

You can set the severity level of the messages to control the type of messages displayed on the consoles and each of the destinations. You can time-stamp log messages or set the syslog source address to enhance real-time debugging and management. For information on possible messages, see the system message guide for this release.

You can access logged system messages by using the switch command-line interface (CLI) or by saving them to a properly configured syslog server. The switch software saves syslog messages in an internal buffer on a standalone switch. If a standalone switch , the log is lost unless you had saved it to flash memory.

You can remotely monitor system messages by viewing the logs on a syslog server or by accessing the switch through Telnet, through the console port, or through the Ethernet management port.

Note The syslog format is compatible with 4.3 BSD UNIX.

System Log Message Format

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or time-stamp information, if configured. Depending on the switch, messages appear in one of these formats:

- *seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n)*
- *seq no:timestamp: %facility-severity-MNEMONIC:description*

The part of the message preceding the percent sign depends on the setting of these global configuration commands:

- **service sequence-numbers**
- **service timestamps log datetime**
- **service timestamps log datetime** [**localtime**] [**msec**] [**show-timezone**]
- **service timestamps log uptime**

Table 107: System Log Message Elements

Element	Description
seq no:	Stamps log messages with a sequence number only if the **service sequence-numbers** global configuration command is configured.
timestamp formats: *mm/dd h h:mm:ss* or *hh:mm:ss* (short uptime) or *d h* (long uptime)	Date and time of the message or event. This information appears only if the **service timestamps log** [**datetime** | **log**] global configuration command is configured.
facility	The facility to which the message refers (for example, SNMP, SYS, and so forth).
severity	Single-digit code from 0 to 7 that is the severity of the message.
MNEMONIC	Text string that uniquely describes the message.

Element	Description
description	Text string containing detailed information about the event being reported.
hostname-n	Hostname of a stack member and its switch number in the stack. Though the is a stack member, it does *not* append its hostname to system messages.

Default System Message Logging Settings

Table 108: Default System Message Logging Settings

Feature	Default Setting
System message logging to the console	Enabled.
Console severity	Debugging.
Logging file configuration	No filename specified.
Logging buffer size	4096 bytes.[19]
Logging history size	1 message.
Time stamps	Disabled.
Synchronous logging	Disabled.
Logging server	Disabled.
Syslog server IP address	None configured.
Server facility	Local7
Server severity	Informational.

[19] For Cisco IOS XE 3.6E release, the default logging buffer size is 16384 bytes.

Syslog Message Limits

If you enabled syslog message traps to be sent to an SNMP network management station by using the **snmp-server enable trap** global configuration command, you can change the level of messages sent and stored in the switch history table. You also can change the number of messages that are stored in the history table.

Messages are stored in the history table because SNMP traps are not guaranteed to reach their destination. By default, one message of the level **warning** and numerically lower levels are stored in the history table even if syslog traps are not enabled.

When the history table is full (it contains the maximum number of message entries specified with the **logging history size** global configuration command), the oldest message entry is deleted from the table to allow the new message entry to be stored.

The history table lists the level keywords and severity level. For SNMP usage, the severity level values increase by 1. For example, *emergencies* equal 1, not 0, and *critical* equals 3, not 2.

Enabling Syslog Trap Messages

You can enable Syslog traps using the **snmp-server enable traps syslog** command.

After enabling Syslog traps, you have to specify the trap message severity. Use the **logging snmp-trap** command to specify the trap level. By default, the command enables severity 0 to 4. To enable all the severity level, configure the **logging snmp-trap 0 7** command.

To enable individual trap levels, configure the following commands:

- **logging snmp-trap emergencies**:Enables only severity 0 traps.
- **logging snmp-trap alert** Enables only severity 1 traps.

Note that, along with the Syslog traps, the Syslog history should also be applied. Without this configuration, Syslog traps are not sent.

Use the **logging history informational** command to enable the Syslog history.

How to Configure System Message Logs

Setting the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console.

This task is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**logging buffered** [*size*] **Example:** `Switch(config)# logging buffered 8192`	Logs messages to an internal buffer on the switch or on a standalone switch or, in the case of a switch stack, on the . The range is 4096 to 2147483647 bytes. The default buffer size is 4096 bytes. If a standalone switch or the fails, the log file is lost unless you previously saved it to flash memory. See Step 4.

	Command or Action	Purpose
		Note Do not make the buffer size too large because the switch could run out of memory for other tasks. Use the **show memory** privileged EXEC command to view the free processor memory on the switch. However, this value is the maximum available, and the buffer size should *not* be set to this amount.
Step 3	**logging** *host* **Example:** `Switch(config)# logging 125.1.1.100`	Logs messages to a UNIX syslog server host. *host* specifies the name or IP address of the host to be used as the syslog server. To build a list of syslog servers that receive logging messages, enter this command more than once.
Step 4	**logging file flash:** *filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*] **Example:** `Switch(config)# logging file flash:log_msg.txt 40960 4096 3`	Stores log messages in a file in flash memory on a standalone switch or, in the case of a switch stack, on the . • *filename*—Enters the log message filename. • (Optional) **max-file-size** —Specifies the maximum logging file size. The range is 4096 to 2147483647. The default is 4096 bytes. • (Optional) *min-file-size*—Specifies the minimum logging file size. The range is 1024 to 2147483647. The default is 2048 bytes. • (Optional) *severity-level-number* | *type*—Specifies either the logging severity level or the logging type. The severity range is 0 to 7.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**terminal monitor** **Example:** `Switch# terminal monitor`	Logs messages to a nonconsole terminal during the current session. Terminal parameter-setting commands are set locally and do not remain in effect after the

	Command or Action	Purpose
		session has ended. You must perform this step for each session to see the debugging messages.

Synchronizing Log Messages

You can synchronize unsolicited messages and **debug** privileged EXEC command output with solicited device output and prompts for a specific console port line or virtual terminal line. You can identify the types of messages to be output asynchronously based on the level of severity. You can also configure the maximum number of buffers for storing asynchronous messages for the terminal after which messages are dropped.

When synchronous logging of unsolicited messages and **debug** command output is enabled, unsolicited device output appears on the console or printed after solicited device output appears or is printed. Unsolicited messages and **debug** command output appears on the console after the prompt for user input is returned. Therefore, unsolicited messages and **debug** command output are not interspersed with solicited device output and prompts. After the unsolicited messages appear, the console again displays the user prompt.

This task is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**line** [**console** | **vty**] *line-number* [*ending-line-number*] **Example:** `Switch(config)# line console`	Specifies the line to be configured for synchronous logging of messages. • **console** —Specifies configurations that occur through the switch console port or the Ethernet management port. • **line vty** *line-number*—Specifies which vty lines are to have synchronous logging enabled. You use a vty connection for configurations that occur through a Telnet session. The range of line numbers is from 0 to 15. You can change the setting of all 16 vty lines at once by entering: line vty 0 15 You can also change the setting of the single vty line being used for your current connection. For example, to change the setting for vty line 2, enter:

	Command or Action	Purpose
		line vty 2 When you enter this command, the mode changes to line configuration.
Step 3	**logging synchronous** [**level** [*severity-level* | **all**] | **limit** *number-of-buffers*] **Example:** `Switch(config)# logging synchronous level 3 limit 1000`	Enables synchronous logging of messages. • (Optional) **level** *severity-level*—Specifies the message severity level. Messages with a severity level equal to or higher than this value are printed asynchronously. Low numbers mean greater severity and high numbers mean lesser severity. The default is 2. • (Optional) **level all**—Specifies that all messages are printed asynchronously regardless of the severity level. • (Optional) **limit** *number-of-buffers*—Specifies the number of buffers to be queued for the terminal after which new messages are dropped. The range is 0 to 2147483647. The default is 20.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Disabling Message Logging

Message logging is enabled by default. It must be enabled to send messages to any destination other than the console. When enabled, log messages are sent to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages.

Disabling the logging process can slow down the switch because a process must wait until the messages are written to the console before continuing. When the logging process is disabled, messages appear on the console as soon as they are produced, often appearing in the middle of command output.

The **logging synchronous** global configuration command also affects the display of messages to the console. When this command is enabled, messages appear only after you press **Return**.

To reenable message logging after it has been disabled, use the **logging on** global configuration command.

This task is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**no logging console** **Example:** `Switch(config)# no logging console`	Disables message logging.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Enabling and Disabling Time Stamps on Log Messages

By default, log messages are not time-stamped.

This task is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 2	Use one of these commands:
	• **service timestamps log uptime**
	• **service timestamps log datetime**[**msec** | **localtime** | **show-timezone**]
	Example:
	`Switch(config)# service timestamps log uptime`
	or
	`Switch(config)# service timestamps log datetime`
		Enables log time stamps.
		• **log uptime**—Enables time stamps on log messages, showing the time since the system was rebooted.
		• **log datetime**—Enables time stamps on log messages. Depending on the options selected, the time stamp can include the date, time in milliseconds relative to the local time zone, and the time zone name.

	Command or Action	Purpose
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Enabling and Disabling Sequence Numbers in Log Messages

If there is more than one log message with the same time stamp, you can display messages with sequence numbers to view these messages. By default, sequence numbers in log messages are not displayed.

This task is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**service sequence-numbers** **Example:** `Switch(config)# service sequence-numbers`	Enables sequence numbers.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Defining the Message Severity Level

Limit messages displayed to the selected device by specifying the severity level of the message.

This task is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Switch# configure terminal`	
Step 2	**logging console** *level* **Example:** `Switch(config)# logging console 3`	Limits messages logged to the console. By default, the console receives debugging messages and numerically lower levels.
Step 3	**logging monitor** *level* **Example:** `Switch(config)# logging monitor 3`	Limits messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels.
Step 4	**logging trap** *level* **Example:** `Switch(config)# logging trap 3`	Limits messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Limiting Syslog Messages Sent to the History Table and to SNMP

This task explains how to limit syslog messages that are sent to the history table and to SNMP.

This task is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**logging history** *level* **Example:** `Switch(config)# logging history 3`	Changes the default level of syslog messages stored in the history file and sent to the SNMP server. By default, **warnings**, **errors**, **critical**, **alerts**, and **emergencies** messages are sent.

	Command or Action	Purpose
Step 3	**logging history size** *number* **Example:** `Switch(config)# logging history size 200`	Specifies the number of syslog messages that can be stored in the history table. The default is to store one message. The range is 0 to 500 messages.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Logging Messages to a UNIX Syslog Daemon

This task is optional.

Note Some recent versions of UNIX syslog daemons no longer accept by default syslog packets from the network. If this is the case with your system, use the UNIX **man syslogd** command to decide what options must be added to or removed from the syslog command line to enable logging of remote syslog messages.

Before you begin

- Log in as root.
- Before you can send system log messages to a UNIX syslog server, you must configure the syslog daemon on a UNIX server.

Procedure

	Command or Action	Purpose
Step 1	Add a line to the file /etc/syslog.conf. **Example:** **local7.debug /usr/adm/logs/***cisco.log*	• **local7**—Specifies the logging facility. • **debug**—Specifies the syslog level. The file must already exist, and the syslog daemon must have permission to write to it.

Step 2	Enter these commands at the UNIX shell prompt.
	Example:
	`$ touch /var/log/cisco.log`
	`$ chmod 666 /var/log/cisco.log`
		Creates the log file. The syslog daemon sends messages at this level or at a more severe level to this file.

	Command or Action	Purpose
Step 3	Make sure the syslog daemon reads the new changes. **Example:** `$ kill -HUP `cat /etc/syslog.pid``	For more information, see the **man syslog.conf** and **man syslogd** commands on your UNIX system.

Monitoring and Maintaining System Message Logs

Monitoring Configuration Archive Logs

Command	Purpose
show archive log config {**all** | **number** [*end-number*] | **user** *username* [**session** *number*] *number* [*end-number*] | **statistics**} [**provisioning**]	Displays the entire configuration log or the log for specified parameters.

Configuration Examples for System Message Logs

Example: Switch System Message

This example shows a partial switch system message on a switch:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
 to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

Additional References for System Message Logs

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference (Catalyst 3850 Switches)System Management Command Reference (Cisco WLC 5700 Series)*
Platform-independent command references	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*
Platform-independent configuration information	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3850 Switches)* *IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

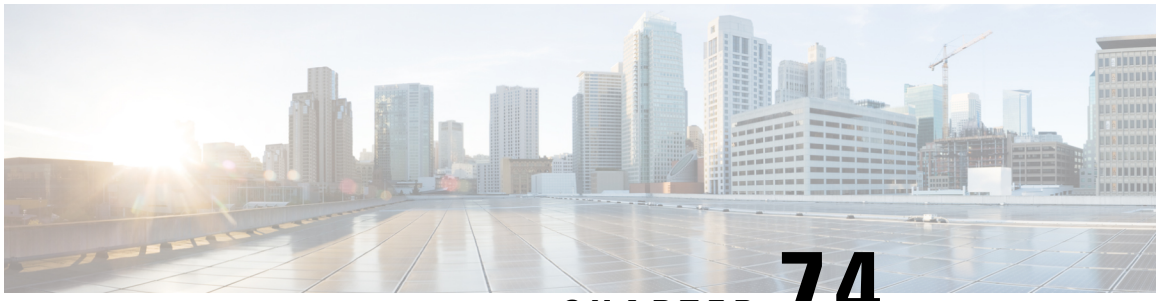
MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For System Message Logs

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 74

Configuring Online Diagnostics

Information About Configuring Online Diagnostics

Online Diagnostics

With online diagnostics, you can test and verify the hardware functionality of the Switch while the Switch is connected to a live network.

The online diagnostics contain packet switching tests that check different hardware components and verify the data path and the control signals.

The online diagnostics detect problems in these areas:

- Hardware components
- Interfaces (Ethernet ports and so forth)
- Solder joints

Online diagnostics are categorized as on-demand, scheduled, or health-monitoring diagnostics. On-demand diagnostics run from the CLI; scheduled diagnostics run at user-designated intervals or at specified times when the Switch is connected to a live network; and health-monitoring runs in the background with user-defined intervals. By default, the health-monitoring test runs for every 30 seconds.

After you configure online diagnostics, you can manually start diagnostic tests or display the test results. You can also see which tests are configured for the Switch or switch stack and the diagnostic tests that have already run.

How to Configure Online Diagnostics

Starting Online Diagnostic Tests

After you configure diagnostic tests to run on the Switch, use the **diagnostic start** privileged EXEC command to begin diagnostic testing.

After starting the tests, you cannot stop the testing process.

Use this privileged EXEC command to manually start online diagnostic testing:

Procedure

	Command or Action	Purpose
Step 1	**diagnostic start switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **complete** | **minimal** | **non-disruptive** | **per-port**} **Example:** `Switch# diagnostic start switch 2 test basic`	Starts the diagnostic tests. You can specify the tests by using one of these options: • *name*—Enters the name of the test. • *test-id*—Enters the ID number of the test. • *test-id-range*—Enters the range of test IDs by using integers separated by a comma and a hyphen. • **all**—Starts all of the tests. • **basic**— Starts the basic test suite. • **complete**—Starts the complete test suite. • **minimal**—Starts the minimal bootup test suite. • **non-disruptive**—Starts the non-disruptive test suite. • **per-port**—Starts the per-port test suite.

Configuring Online Diagnostics

You must configure the failure threshold and the interval between tests before enabling diagnostic monitoring.

Scheduling Online Diagnostics

You can schedule online diagnostics to run at a designated time of day or on a daily, weekly, or monthly basis for a Switch. Use the **no** form of this command to remove the scheduling.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**diagnostic schedule switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **complete** | **minimal** | **non-disruptive** | **per-port**} {**daily** | **on** *mm dd yyyy hh:mm* | **port** *inter-port-number port-number-list* | **weekly** *day-of-week hh:mm*} **Example:** `Switch(config)# diagnostic schedule switch 3 test 1-5 on July 3 2013 23:10`	Schedules on-demand diagnostic tests for a specific day and time. When specifying the tests to be scheduled, use these options: • *name*—Name of the test that appears in the **show diagnostic content** command output. • *test-id*—ID number of the test that appears in the **show diagnostic content** command output. • *test-id-range*—ID numbers of the tests that appear in the **show diagnostic content** command output. • **all**—All test IDs. • **basic**—Starts the basic on-demand diagnostic tests. • **complete**—Starts the complete test suite. • **minimal**—Starts the minimal bootup test suite. • **non-disruptive**—Starts the non-disruptive test suite. • **per-port**—Starts the per-port test suite. You can schedule the tests as follows: • Daily—Use the **daily** *hh:mm* parameter. • Specific day and time—Use the **on** *mm dd yyyy hh:mm* parameter. • Weekly—Use the **weekly** *day-of-week hh:mm* parameter.

Configuring Health-Monitoring Diagnostics

You can configure health-monitoring diagnostic testing on a Switch while it is connected to a live network. You can configure the execution interval for each health-monitoring test, enable the Switch to generate a syslog message because of a test failure, and enable a specific test.

Use the **no** form of this command to disable testing.

By default, health monitoring is disabled, but the Switch generates a syslog message when a test fails.

Follow these steps to configure and enable the health-monitoring diagnostic tests:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**diagnostic monitor interval switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds day* **Example:** `Switch(config)# diagnostic monitor interval switch 2 test 1 12:30:00 750 5`	Configures the health-monitoring interval of the specified tests. When specifying the tests, use one of these parameters: • *name*—Name of the test that appears in the **show diagnostic content** command output. • *test-id*—ID number of the test that appears in the **show diagnostic content** command output. • *test-id-range*—ID numbers of the tests that appear in the **show diagnostic content** command output. • **all**—All of the diagnostic tests. When specifying the interval, set these parameters: • *hh:mm:ss*—Monitoring interval in hours, minutes, and seconds. The range for *hh* is 0 to 24, and the range for *mm* and *ss* is 0 to 60.

	Command or Action	Purpose
		• *milliseconds*—Monitoring interval in milliseconds (ms). The range is from 0 to 999. • *day*—Monitoring interval in the number of days. The range is from 0 to 20.
Step 4	**diagnostic monitor syslog** **Example:** `Switch(config)# diagnostic monitor syslog`	(Optional) Configures the switch to generate a syslog message when a health-monitoring test fails.
Step 5	**diagnostic monitor threshold switch** *number number* **test** {*name* | *test-id* | *test-id-range* | **all**} **failure count** *count* **Example:** `Switch(config)# diagnostic monitor threshold switch 2 test 1 failure count 20`	(Optional) Sets the failure threshold for the health-monitoring tests. When specifying the tests, use one of these parameters: • *name*—Name of the test that appears in the **show diagnostic content** command output. • *test-id*—ID number of the test that appears in the **show diagnostic content** command output. • *test-id-range*—ID numbers of the tests that appear in the **show diagnostic content** command output. • **all**—All of the diagnostic tests. The range for the failure threshold *count* is 0 to 99.
Step 6	**diagnostic monitor switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all**} **Example:** `Switch(config)# diagnostic monitor switch 2 test 1`	Enables the specified health-monitoring tests. The **switch** *number* keyword is supported only on stacking switches. When specifying the tests, use one of these parameters: • *name*—Name of the test that appears in the **show diagnostic content** command output. • *test-id*—ID number of the test that appears in the **show diagnostic content** command output.

	Command or Action	Purpose
		• *test-id-range*—ID numbers of the tests that appear in the **show diagnostic content** command output. • **all**—All of the diagnostic tests.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 8	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 9	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

Use the **no diagnostic monitor interval test***test-id* | *test-id-range* } global configuration command to change the interval to the default value or to zero. Use the **no diagnostic monitor syslog** command to disable generation of syslog messages when a health-monitoring test fails. Use the **diagnostic monitor threshold test***test-id* | *test-id-range* }**failure count**command to remove the failure threshold.

Monitoring and Maintaining Online Diagnostics

Displaying Online Diagnostic Tests and Test Results

You can display the online diagnostic tests that are configured for the Switch or Switch stack and check the test results by using the privileged EXEC **show** commands in this table:

Table 109: Commands for Diagnostic Test Configuration and Results

Command	Purpose
show diagnostic content switch [*number* | **all**]	Displays the online diagnostics configured for a switch.
show diagnostic status	Displays the currently running diagnostic tests.

Command	Purpose
show diagnostic result switch [*number* | **all**] [**detail** | **test** {*name* | *test-id* | *test-id-range* | **all**} [**detail**]]	Displays the online diagnostics test results.
show diagnostic switch [*number* | **all**] [**detail**]	Displays the online diagnostics test results.
show diagnostic schedule switch [*number* | **all**]	Displays the online diagnostics test schedule.
show diagnostic post	Displays the POST results. (The output is the same as the **show post** command output.)

Configuration Examples for Online Diagnostic Tests

Examples: Start Diagnostic Tests

This example shows how to start a diagnostic test by using the test name:

```
Switch# diagnostic start switch 2 test TestInlinePwrCtlr
```

This example shows how to start all of the basic diagnostic tests:

```
Switch# diagnostic start switch 1 test all
```

Example: Configure a Health Monitoring Test

This example shows how to configure a health-monitoring test:

```
Switch(config)# diagnostic monitor threshold switch 1 test 1 failure count 50
Switch(config)# diagnostic monitor interval switch 1 test TestPortAsicStackPortLoopback
```

Examples: Schedule Diagnostic Test

This example shows how to schedule diagnostic testing for a specific day and time on a specific switch:

```
Switch(config)# diagnostic schedule test DiagThermalTest on June 3 2013  22:25
```

This example shows how to schedule diagnostic testing to occur weekly at a certain time on a specific switch:

```
Switch(config)# diagnostic schedule switch 1 test 1,2,4-6 weekly saturday 10:30
```

Examples: Displaying Online Diagnostics

This example shows how to display on demand diagnostic settings:

```
Switch# show diagnostic ondemand settings

Test iterations = 1
Action on test failure = continue
```

This example shows how to display diagnostic events for errors:

```
Switch# show diagnostic events event-type error

Diagnostic events (storage for 500 events, 0 events recorded)
Number of events matching above criteria = 0

No diagnostic log entry exists.
```

This example shows how to display the description for a diagnostic test:

```
Switch# show diagnostic description switch 1 test all

DiagGoldPktTest :
        The GOLD packet Loopback test verifies the MAC level loopback
        functionality. In this test, a GOLD packet, for which doppler
        provides the support in hardware, is sent. The packet loops back
        at MAC level and is matched against the stored packet. It is a non
        -disruptive test.

DiagThermalTest :
        This test verifies the temperature reading from the sensor is below the yellow
        temperature threshold. It is a non-disruptive test and can be run as a health
monitoring test.

DiagFanTest :
        This test verifies all fan modules have been inserted and working properly on the
board
        It is a non-disruptive test and can be run as a health monitoring test.

DiagPhyLoopbackTest :
        The PHY Loopback test verifies the PHY level loopback
        functionality. In this test, a packet is sent which loops back
        at PHY level and is matched against the stored packet. It is a
        disruptive test and cannot be run as a health monitoring test.

DiagScratchRegisterTest :
        The Scratch Register test monitors the health of application-specific
        integrated circuits (ASICs) by writing values into registers and reading
        back the values from these registers. It is a non-disruptive test and can
        be run as a health monitoring test.

DiagPoETest :
        This test checks the PoE controller functionality. This is a disruptive test
        and should not be performed during normal switch operation.


DiagMemoryTest :
        This test runs the exhaustive ASIC memory test during normal switch operation
        NG3K utilizes mbist for this test. Memory test is very disruptive
        in nature and requires switch reboot after the test.
```

```
Switch#
```

This example shows how to display the boot up level:

```
Switch# show diagnostic bootup level

Current bootup diagnostic level: minimal

Switch#
```

Additional References for Online Diagnostics

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference (Catalyst 3850 Switches)System Management Command Reference (Cisco WLC 5700 Series)*
Platform-independent command reference	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*
Platform-independent configuration information	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

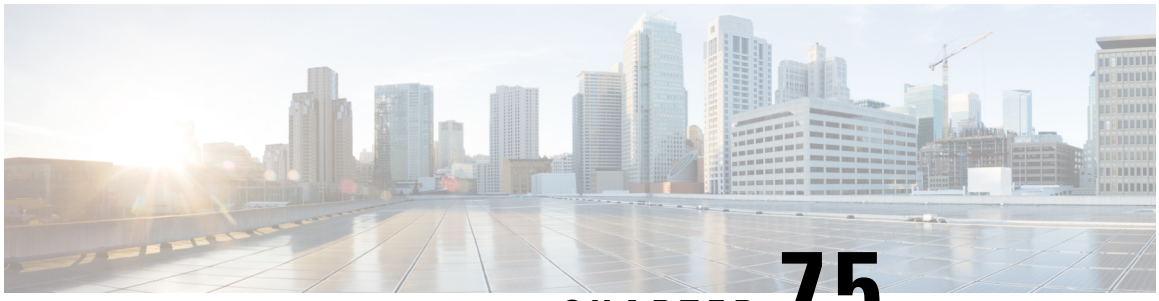
MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for Configuring Online Diagnostics

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 75

Predownloading an Image to Access Points

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Predownloading an Image to an Access Point

To minimize network outages, you can now download an upgrade image to the access point from the switch without resetting the access point or losing network connectivity. Previously, you would download an upgrade image to the switch and reset it, which causes the access point to go into discovery mode. After the access point discovers the controller with the new image, the access point downloads the new image, resets, goes into discovery mode, and rejoins the switch.

You can now download the upgrade image to the switch and then download the image to the access point while the network is still up. When both devices are up, the access point discovers and rejoins the switch.

Restrictions for Predownloading an Image to an Access Point

The following are the restrictions for predownloading an image to an access point:

- The maximum number of concurrent predownloads is limited to half the number of concurrent normal image downloads. This limitation allows new access points to join the controller during image downloading.

  If you reach the predownload limit, then the access points that cannot get an image sleep for a time between 180 to 600 seconds and then reattempt the predownload.
- Access points with 16-MB total available memory may not have enough free memory to download an upgrade image and may automatically delete crash info files, radio files, and any backup images to free up space. However, this limitation does not affect the predownload process because the predownload image replaces any backup image on the access point.
- All of the primary, secondary, and tertiary controllers should run the same images or the feature will not be effective.
- At the time of reset, you must make sure that all of the access points have downloaded the image.
- The access point can store only two software images.

How to Predownload an Image to an Access Point

Predownloading an Image to Access Points (CLI)

Before you begin

There are some prerequisites that you must keep in mind while predownloading an image to an access point:

- Predownloading can be done only when the switch is booted in the install mode.
- You can copy the new image either from the TFTP server, flash image, or USB.
- Before predownloading the new image, you must install the new software using the **software install** command and select **no** to the **reload** option.
- If the latest upgrade image is already present in the AP, predownload will not be triggered. Check whether the primary and backup image versions are the same as upgrade image using the **show ap image** command.

Procedure

	Command or Action	Purpose

Step 1	**ap image predownload** or **ap** *ap-name* **image predownload**
	Example:
	`Switch# ap image predownload`
	`Switch#`
		Downloads the new image to all access points or a specific access point connected to the switch.

Step 2	**show ap image** **Example:** `Switch# show ap image`	Verifies the access points predownload status. This command will initially display the status as "Predownloading" and then move to "Completed", when download is complete.

	Command or Action	Purpose
Step 3	**Example:** `Switch# ap image swap`	Swaps the images of APs that has completed predownload.
Step 4	**ap image reset** **Example:** `Switch# ap image reset`	Resets the access points.
Step 5	**reload** **Example:** `Switch# reload`	Resets the system.

Monitoring Access Point Predownload Process

This section describes the command for monitoring the access point predownload process.

The following command can be used to monitor the access point predownload process: **show ap image**

Displaying Access Point Predownload Status

While downloading the access point predownload image, you can simultaneously enter the **show ap image** command to verify the predownload progress on the access points:

```
Switch# show ap image
Total number of APs  : 1

Number of APs
       Initiated                : 1
       Predownloading           : 1
       Completed predownloading   : 0
       Not Supported            : 0
       Failed to Predownload      : 0

AP Name                         Primary Image   Backup Image    Predownload Status
Predownload Ver...  Next Retry Time    Retry Count
-----------------------------------------------------------------------------------
AP1                             10.0.1.66       10.0.1.66       Predownloading
10.0.1.67           NA                          0


Switch# show ap image

Total number of APs  : 1

Number of APs
       Initiated                : 1
       Predownloading           : 0
       Completed predownloading   : 1
       Not Supported            : 0
       Failed to Predownload      : 0

AP Name                         Primary Image   Backup Image    Predownload Status
Predownload Ver...  Next Retry Time    Retry Count
-----------------------------------------------------------------------------------
```

```
AP1                                 10.0.1.66       10.0.1.67       Complete
10.0.1.67           NA                              0
```

The following command can be used to view image details of a particular AP:

```
Switch# show ap name APe4aa.5dd1.99b0 image

AP Name : APe4aa.5dd1.99b0
Primary Image : 16.6.230.46
Backup Image : 3.0.51.0
Predownload Status : None
Predownload Version : 000.000.000.000
Next Retry Time : N/A
Retry Count : 0
```

Examples: Access Point Predownload Process

This example shows how to predownload an image to an access point AP1:

```
Switch# ap image predownload
Switch# show ap image
Switch# ap image swap
Switch# show ap image
Switch# ap image reset
Switch# reload
```

Additional References for Predownloading an Image to an Access Point

Related Documents

Related Topic	Document Title
Lightweight access points configuration	
Lightweight Access Point commands	

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

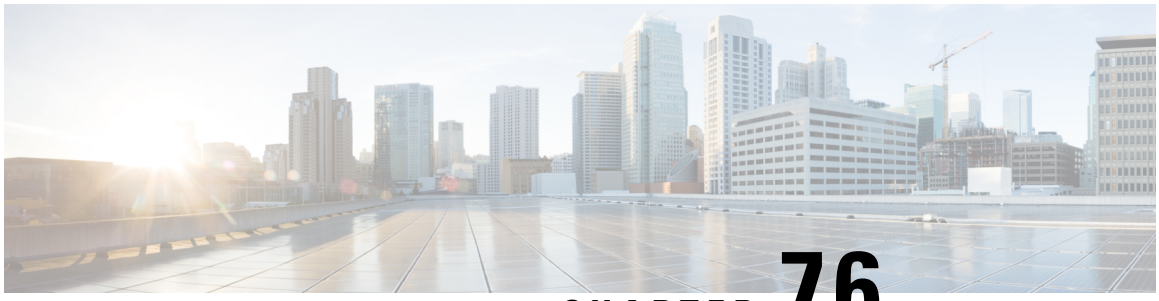
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Performing Predownloading an Image to an Access Point

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 76

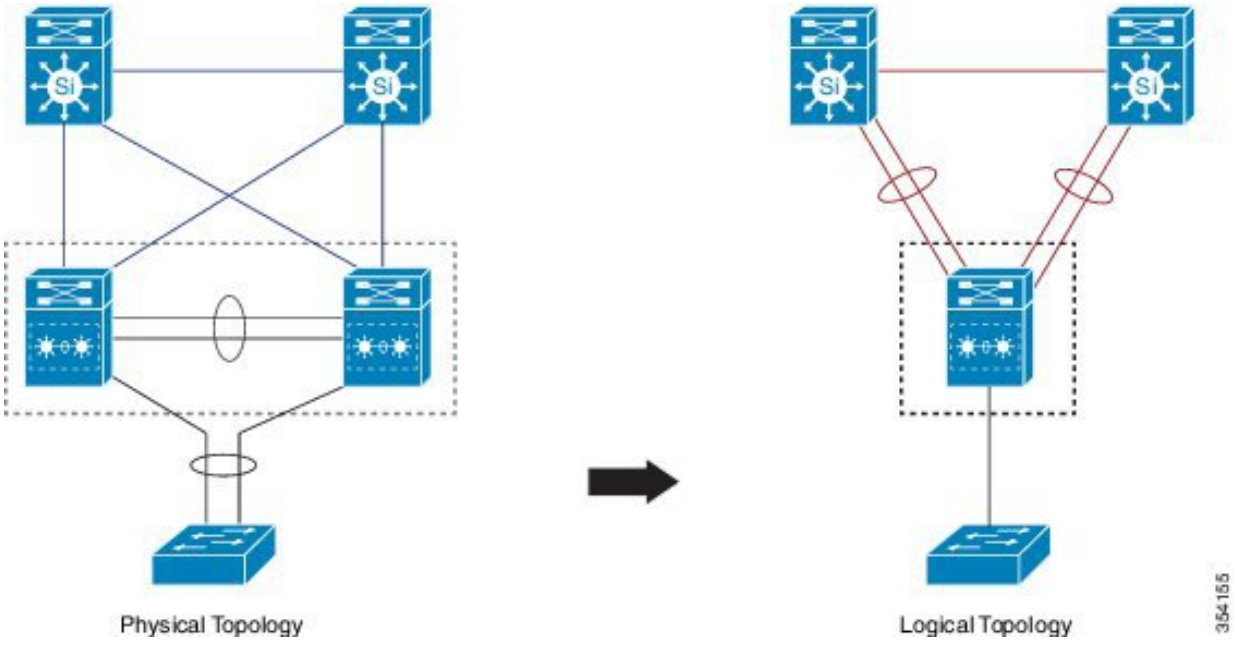
Configuring Wireless Virtual Switching System

Information About Wireless Virtual Switching System

The Cisco Wireless Virtual Switching System (VSS) is a clustering technology that pools two Cisco Catalyst 4500-E Series Switches into a single virtual switch. In a VSS, the data plane of both the clustered switches are active at the same time in both the chassis. VSS members are connected by virtual switch links (VSLs) using connections between the VSS members. VSLs can carry regular user traffic in addition to the control plane communication between the VSS members.

Note We recommend that you use 10-Gigabit Ethernet links for a VSL bundle.

Figure 71: Physical vs Logical Topology in a VSS Configuration



The Cisco Catalyst 4500E Supervisor 8-E Switch supports wireless in VSS. It can be operated as a mobility agent (MA) or mobility controller (MC). An MA maintains Control and Provisioning of Wireless Access Points (CAPWAP) tunnels of directly connected access points and client mobility state machine. An MC provides mobility management services for group roaming events.

MA and MC can be co-located on the same switch. AP-count licenses are used only when the switch is in MC mode. The MC is the gatekeeper for tracking the AP-count licenses and decides whether an access point can be included in or not.

Note All the features supported in the wireless mode on a stand-alone chassis are also supported in the wireless VSS mode.

For more information on VSS, see the following guide: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/XE3-7-0E/15-23E/configuration/guide/xe-370-configuration/vss.html

VSS Conversion Methods

The wireless VSS can be deployed in a network using any of the following methods:

- Migrating the wired VSS to wireless VSS.
- Migrating the existing wireless network to a wireless VSS network.

Restrictions

The wireless VSS feature is supported on Cisco Wireless LAN Controller (WLC) with the following restrictions:

- Multiple APs per port are not supported.

- The wireless VSS feature is not supported by Cisco Prime Infrastructure on Cisco IOS XE 3.8.0.
- The supervisors cannot be booted in any other mode except the wireless mode.

Related Topics

Configuring VSS for the Cisco Catalyst 4500 Series Switch (Supervisor Engine 8-E), on page 1401
Verifying DC Bootup with VSS, on page 1403

Configuring VSS for the Cisco Catalyst 4500 Series Switch (Supervisor Engine 8-E)

The Cisco Wireless Virtual Switching System (VSS) is a clustering technology that pools two Cisco Catalyst 4500-E Series Switches into a single virtual switch. In a VSS, the data plane of both clustered switches are active at the same time in both the chassis. VSS members are connected by virtual switch links (VSLs) using connections between the VSS members. VSLs can carry regular user traffic in addition to the control plane communication between the VSS members.

Procedure

Step 1 Assign the virtual switch domain and switch number.

Configure the same virtual switch domain number on both switches of the VSS. The virtual switch domain is a number between 1 and 255. After configuring the domain number, configure one switch as switch number 1 and the other switch as switch number 2.

Example:

```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# switch virtual domain 10
Domain ID 10 config will take effect only after the exec command 'switch convert mode
virtual' is issued
SW1(config-vs-domain)# switch 1
SW1(config-vs-domain)# exit

SW2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)# switch virtual domain 10
Domain ID 10 config will take effect only after the exec command 'switch convert mode
virtual' is issued
SW2(config-vs-domain)# switch 2
SW2(config-vs-domain)# exit
```

Step 2 Configure the VSL port channel.

Configure VSL with a unique port channel on each switch. During the conversion, the VSS configures both the port channels on the VSS active switch. If the VSS standby switch's VSL port channel number has been configured for another use, the VSS comes up in RPR mode. To avoid this situation, check whether both the port channel numbers are available on both the switches.

Example:

```
SW1(config)# interface port-channel 5
SW1(config-if)# switchport
SW1(config-if)# switch virtual link 1
SW1(config-if)# no shut
SW1(config-if)# exit


SW2(config)# interface port-channel 10
SW2(config-if)# switchport
SW2(config-if)# switch virtual link 2
SW2(config-if)# no shut
SW2(config-if)# exit
```

Step 3 Configure VSL ports.

Add the VSL physical ports to the port-channel. In the following example, interfaces TenGigabitEthernet 1/1 and 1/2 on Switch 1 are connected to interfaces TenGigabitEthernet 1/1 and 1/2 on Switch 2.

Note After the interfaces are included in the VSL port-channel with channel-group command, the interfaces moves to the "notconnect" status. The interface status will be up, but the line protocol will be down. The interface will be in UP/down (notconnect) status, till the switch is rebooted in step 4.

Example:

```
SW1(config)# interface range Te1/1 - 2
SW1(config-if-range)# switchport mode trunk
SW1(config-if-range)# channel-group 5 mode on
WARNING: Interface TenGigabitEthernet1/1 placed in restricted config mode. All extraneous
configs removed!
WARNING: Interface TenGigabitEthernet1/2 placed in restricted config mode. All extraneous
configs removed!
SW1(config-if-range)# exit

SW2(config)# interface range Te1/1 - 2
SW2(config-if-range)# switchport mode trunk
SW2(config-if-range)# channel-group 10 mode on
WARNING: Interface TenGigabitEthernet1/1 placed in restricted config mode. All extraneous
configs removed!
WARNING: Interface TenGigabitEthernet1/2 placed in restricted config mode. All extraneous
configs removed!
SW2(config-if-range)# exit
```

Step 4 Convert the Switch to VSS.

Enter the switch convert mode virtual command on Switch 1 for converting switch's mode to Virtual Switch Mode. Enter your confirmation at the next prompt. The system creates a converted configuration file, and saves the file to bootflash.

Example:

```
SW1# switch convert mode virtual

This command will convert all interface names to naming convention "interface-type
switch-number/slot/port",save the running config to startup-config and reload the switch.
Do you want to proceed? [yes/no]: yes
Converting interface names
Building configuration...
Compressed configuration from 6551 bytes to 2893 bytes[OK]
Saving converted configuration to bootflash: ...
```

```
Destination filename [startup-config.converted_vs-20130124-062921]?
Please stand by while rebooting the system...
Restarting system.

Rommon (G) Signature verification PASSED
Rommon (P) Signature verification PASSED
FPGA   (P) Signature verification PASSED

!Enter the switch convert mode virtual command on Switch 2 for converting the switch's mode
 to Virtual Switch Mode.

SW2# switch convert mode virtual

This command will convert all interface names to naming convention "interface-type
switch-number/slot/port",save the running config to startup-config andreload the switch.
Do you want to proceed? [yes/no]: yes
Converting interface names
Building configuration...
Compressed configuration from 6027 bytes to 2774 bytes[OK]
Saving converted configuration to bootflash: ...
Destination filename [startup-config.converted_vs-20130124-052526]?
Please stand by while rebooting the system...
Restarting system.

Rommon (G) Signature verification PASSED
Rommon (P) Signature verification PASSED
FPGA   (P) Signature verification PASSED
```

Related Topics

Information About Wireless Virtual Switching System, on page 1399
Verifying DC Bootup with VSS, on page 1403

Verifying DC Bootup with VSS

The wireless mode will show dc boot status and errors (if any) during boot up.

```
vss# show module

Switch Number: 1 Role: Virtual Switch Active
Chassis Type : WS-C4507R+E
Power consumed by backplane : 40 Watts

Mod  Ports  Card Type                                  Model              Serial No.
---+-----+--------------------------------------+------------------+------------
1    48     10/100/1000BaseT Premium POE E Series  WS-X4748-RJ45V+E  CAT1737L0B5
4    12     Sup 8-E 10GE (SFP+), 1000BaseX (SFP)   WS-X45-SUP8-E     CAT1746L6B9

M  MAC addresses                    Hw   Fw           Sw               Status
--+---------------------------------+---+------------+----------------+---------
1  885a.9244.1740 to 885a.9244.176f 1.3                                Ok
4  2894.0f2a.404c to 2894.0f2a.4057 1.0 15.1(1r)SG(0 03.08.00.E.91    Ok

Mod  Redundancy role      Operating mode      Redundancy status
----+------------------+------------------+---------------------------------
4    Active Supervisor   SSO                Active

Mod  Submodule               Model             Serial No.  Hw   Status
```

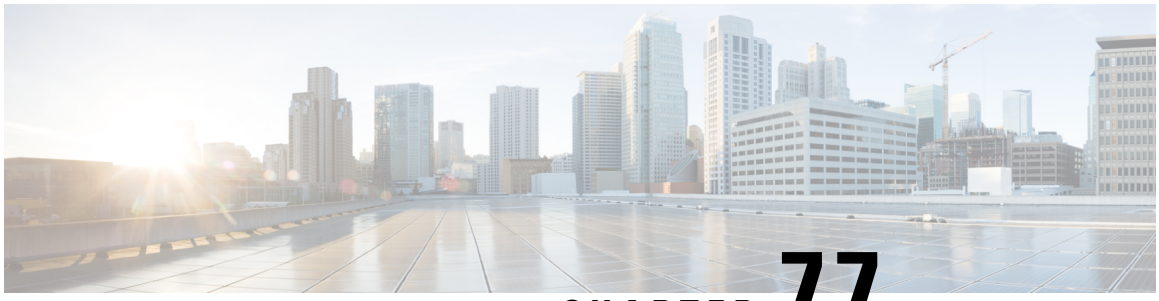
```
----+-----------------------+-----------------+------------+----+---------
4    Daughter Card           WS-UA-SUP8E      CAT1746L6UB   1.0  Ok

Switch Number: 2 Role: Virtual Switch Standby
Chassis Type : WS-C4503-E
Power consumed by backplane : 0 Watts

Mod  Ports  Card Type                              Model              Serial No.
---+-----+--------------------------------------+------------------+------------
1   12 Sup  8-E 10GE (SFP+), 1000BaseX (SFP)      WS-X45-SUP8-E      CAT1731L0PF
3   48      10/100/1000BaseT Premium POE E Series WS-X4748-RJ45V+E   CAT1418L030

M  MAC addresses                    Hw   Fw           Sw               Status
--+--------------------------------+---+------------+----------------+---------
1   001b.2a68.48c0 to 001b.2a68.48cb 1.0 15.1(1r)SG(0 03.08.00.E.91    Ok
3   0026.9927.f310 to 0026.9927.f33f 0.4                               Ok

Mod  Redundancy role     Operating mode      Redundancy status
----+------------------+------------------+----------------------------------
1    Standby              Supervisor  SSO                 Standby hot

Mod   Submodule Model   Serial No.  Hw   Status
```

Related Topics

Information About Wireless Virtual Switching System, on page 1399
Configuring VSS for the Cisco Catalyst 4500 Series Switch (Supervisor Engine 8-E), on page 1401

How to Boot a Switch in Wireless Mode

To boot a switch in wireless mode (this is called the install boot), additional steps are required. For more information, see the Install Boot section of the *Cisco Catalyst 4500 Supervisor Engine 8-E Wireless Mode Quick-Start Guide*at:http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-series-switches/guide-c07-73%203704.html



CHAPTER 77

Troubleshooting the Software Configuration

This chapter describes how to identify and resolve software problems related to the Cisco IOS software on the switch. Depending on the nature of the problem, you can use the command-line interface (CLI), Device Manager, or Network Assistant to identify and solve problems.

Additional troubleshooting information, such as LED descriptions, is provided in the hardware installation guide.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Troubleshooting the Software Configuration

Software Failure on a Switch

Switch software can be corrupted during an upgrade by downloading the incorrect file to the switch, and by deleting the image file. In all of these cases, the switch does not pass the power-on self-test (POST), and there is no connectivity.

Related Topics

Recovering from a Software Failure, on page 1413

Lost or Forgotten Password on a Switch

The default configuration for the switch allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process during power-on and by entering a new password. These recovery procedures require that you have physical access to the switch.

Note On these switches, a system administrator can disable some of the functionality of this feature by allowing an end user to reset a password only by agreeing to return to the default configuration. If you are an end user trying to reset a password when password recovery has been disabled, a status message reminds you to return to the default configuration during the recovery process.

Note You cannot recover encryption password key, when Cisco WLC configuration is copied from one Cisco WLC to another (in case of an RMA).

Related Topics

Recovering from a Lost or Forgotten Password, on page 1415

Power over Ethernet Ports

A Power over Ethernet (PoE) switch port automatically supplies power to one of these connected devices if the switch detects that there is no power on the circuit:

- a Cisco pre-standard powered device (such as a Cisco IP Phone or a Cisco Aironet Access Point)
- an IEEE 802.3af-compliant powered device
- an IEEE 802.3at-compliant powered device

A powered device can receive redundant power when it is connected to a PoE switch port and to an AC power source. The device does not receive redundant power when it is only connected to the PoE port.

After the switch detects a powered device, the switch determines the device power requirements and then grants or denies power to the device. The switch can also detect the real-time power consumption of the device by monitoring and policing the power usage.

For more information, see the "Configuring PoE" chapter in the *Interface and Hardware Component Configuration Guide (Catalyst 3850 Switches) Interface Configuration Guide (Cisco WLC 5700 Series)*.

Related Topics

Scenarios to Troubleshoot Power over Ethernet (PoE), on page 1428

Disabled Port Caused by Power Loss

If a powered device (such as a Cisco IP Phone 7910) that is connected to a PoE Switch port and powered by an AC power source loses power from the AC power source, the device might enter an error-disabled state.

To recover from an error-disabled state, enter the **shutdown** interface configuration command, and then enter the **no shutdown** interface command. You can also configure automatic recovery on the Switch to recover from the error-disabled state.

On a Switch, the **errdisable recovery cause loopback** and the **errdisable recovery interval** *seconds* global configuration commands automatically take the interface out of the error-disabled state after the specified period of time.

Disabled Port Caused by False Link-Up

If a Cisco powered device is connected to a port and you configure the port by using the **power inline never** interface configuration command, a false link-up can occur, placing the port into an error-disabled state. To take the port out of the error-disabled state, enter the **shutdown** and the **no shutdown** interface configuration commands.

You should not connect a Cisco powered device to a port that has been configured with the **power inline never** command.

Ping

The Switch supports IP ping, which you can use to test connectivity to remote hosts. Ping sends an echo request packet to an address and waits for a reply. Ping returns one of these responses:

- Normal response—The normal response (*hostname* is alive) occurs in 1 to 10 seconds, depending on network traffic.
- Destination does not respond—If the host does not respond, a *no-answer* message is returned.
- Unknown host—If the host does not exist, an *unknown host* message is returned.
- Destination unreachable—If the default gateway cannot reach the specified network, a *destination-unreachable* message is returned.
- Network or host unreachable—If there is no entry in the route table for the host or network, a *network or host unreachable* message is returned.

Related Topics

Executing Ping, on page 1422
Example: Pinging an IP Host, on page 1430

Layer 2 Traceroute

The Layer 2 traceroute feature allows the switch to identify the physical path that a packet takes from a source device to a destination device. Layer 2 traceroute supports only unicast source and destination MAC addresses. Traceroute finds the path by using the MAC address tables of the Switch in the path. When the Switch detects a device in the path that does not support Layer 2 traceroute, the Switch continues to send Layer 2 trace queries and lets them time out.

The Switch can only identify the path from the source device to the destination device. It cannot identify the path that a packet takes from source host to the source device or from the destination device to the destination host.

Layer 2 Traceroute Guidelines

- Cisco Discovery Protocol (CDP) must be enabled on all the devices in the network. For Layer 2 traceroute to function properly, do not disable CDP.

  If any devices in the physical path are transparent to CDP, the switch cannot identify the path through these devices.

- A Switch is reachable from another Switch when you can test connectivity by using the **ping** privileged EXEC command. All Switch in the physical path must be reachable from each other.
- The maximum number of hops identified in the path is ten.
- You can enter the **traceroute mac** or the **traceroute mac ip** privileged EXEC command on a Switch that is not in the physical path from the source device to the destination device. All Switch in the path must be reachable from this switch.
- The **traceroute mac** command output shows the Layer 2 path only when the specified source and destination MAC addresses belong to the same VLAN. If you specify source and destination MAC addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.
- If you specify a multicast source or destination MAC address, the path is not identified, and an error message appears.
- If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.
- The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses belong to the same subnet. When you specify the IP addresses, the Switch uses the Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.
  - If an ARP entry exists for the specified IP address, the Switch uses the associated MAC address and identifies the physical path.
  - If an ARP entry does not exist, the Switch sends an ARP query and tries to resolve the IP address. If the IP address is not resolved, the path is not identified, and an error message appears.
- When multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port), the Layer 2 traceroute feature is not supported. When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.
- This feature is not supported in Token Ring VLANs.

IP Traceroute

You can use IP traceroute to identify the path that packets take through the network on a hop-by-hop basis. The command output displays all network layer (Layer 3) devices, such as routers, that the traffic passes through on the way to the destination.

Your Switch can participate as the source or destination of the **traceroute** privileged EXEC command and might or might not appear as a hop in the **traceroute** command output. If the Switch is the destination of the traceroute, it is displayed as the final destination in the traceroute output. Intermediate Switch do not show up in the traceroute output if they are only bridging the packet from one port to another within the same VLAN.

However, if the intermediate Switch is a multilayer Switch that is routing a particular packet, this Switch shows up as a hop in the traceroute output.

The **traceroute** privileged EXEC command uses the Time To Live (TTL) field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a User Datagram Protocol (UDP) datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends an Internet Control Message Protocol (ICMP) time-to-live-exceeded message to the sender. Traceroute finds the address of the first hop by examining the source address field of the ICMP time-to-live-exceeded message.

To identify the next hop, traceroute sends a UDP packet with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the time-to-live-exceeded message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

To learn when a datagram reaches its destination, traceroute sets the UDP destination port number in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram destined to itself containing a destination port number that is unused locally, it sends an ICMP *port-unreachable* error to the source. Because all errors except port-unreachable errors come from intermediate hops, the receipt of a port-unreachable error means that this message was sent by the destination port.

Related Topics

Executing IP Traceroute, on page 1423
Example: Performing a Traceroute to an IP Host, on page 1431

Time Domain Reflector Guidelines

You can use the Time Domain Reflector (TDR) feature to diagnose and resolve cabling problems. When running TDR, a local device sends a signal through a cable and compares the reflected signal to the initial signal.

TDR is supported only on 10/100/1000 copper Ethernet ports. It is not supported on 10-Gigabit Ethernet ports and on SFP module ports.

TDR is supported on 10/100/1000 copper Ethernet ports and on Multigigabit Ethernet (100Mbps/1/2.5/5/10 Gbps) ports. It is not supported on SFP module ports.

TDR can detect these cabling problems:

- Open, broken, or cut twisted-pair wires—The wires are not connected to the wires from the remote device.
- Shorted twisted-pair wires—The wires are touching each other or the wires from the remote device. For example, a shorted twisted pair can occur if one wire of the twisted pair is soldered to the other wire.

  If one of the twisted-pair wires is open, TDR can find the length at which the wire is open.

Note When using the feature with Multigigabit Ethernet ports, the cable length is displayed only when an open or short condition is detected.

Use TDR to diagnose and resolve cabling problems in these situations:

- Replacing a Switch
- Setting up a wiring closet
- Troubleshooting a connection between two devices when a link cannot be established or when it is not operating properly

When you run TDR, the Switch reports accurate information in these situations:

- The cable for the gigabit link is a solid-core cable.
- The open-ended cable is not terminated.

When you run TDR, the Switch does not report accurate information in these situations:

- The cable for the gigabit link is a twisted-pair cable or is in series with a solid-core cable.
- The link is a 10-megabit or a 100-megabit link.
- The cable is a stranded cable.
- The link partner is a Cisco IP Phone.
- The link partner is not IEEE 802.3 compliant.

Debug Commands

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

All **debug** commands are entered in privileged EXEC mode, and most **debug** commands take no arguments.

Related Topics

Redirecting Debug and Error Message Output, on page 1423
Example: Enabling All System Diagnostics, on page 1432

Crashinfo Files

The crashinfo files save information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The switch generates two files at the time of the failure: full core and crashinfo.

The information in the crashinfo file includes the Cisco IOS image name and version that failed, a list of the processor registers, and a stack trace. You can provide this information to the Cisco technical support representative by using the **show tech-support** privileged EXEC command.

The file names have the following format:

```
[fullcore | crashinfo]_[process that crashed]_[date]-[timestamp]-UTC
```

From IOS, you can view the crashinfo files on each switch by using the following command:

```
Switch#  dir crashinfo?
crashinfo-1: crashinfo-2: crashinfo-3: crashinfo:
Switch#
```

For example, to access the crashinfo directory for switch 1, enter

```
Switch dir crashinfo-1
```

From the ROMMON prompt, you can view the crashinfo files by using the **dir** command:

```
Switch: dir sda1
```

The following is sample output of a crashinfo file

```
Switch# dir crashinfo:

Directory of crashinfo:/

   12  -rwx        2768  Dec 31 1969 16:00:15 -08:00  koops.dat
   15  -rwx           0  Jan 12 2000 22:53:40 -08:00  deleted_crash_files
   16  -rwx     4246576  Jan 12 2000 22:53:40 -08:00  crashinfo_stack-mgr_20000113-065250-UTC

   17  -rwx          50   Oct 2 2012 03:18:42 -08:00  last_crashinfo
   26  -rwx          39  Jan 22 2013 14:14:14 -08:00  last_systemreport
   18  -rwx     2866565  Jan 12 2000 22:53:41 -08:00  fullcore_stack-mgr_20000113-065250-UTC

   20  -rwx     4391796   Feb 1 2000 17:50:44 -08:00  crashinfo_stack-mgr_20000202-014954-UTC

   21  -rwx     2920325   Feb 1 2000 17:50:45 -08:00  fullcore_stack-mgr_20000202-014954-UTC
34817  -rw-     1050209  Jan 10 2013 20:26:23 -08:00  system-report_1_20130111-042535-UTC.gz
18434  -rw-     1016913  Jan 11 2013 10:35:28 -08:00  system-report_1_20130111-183440-UTC.gz
18435  -rw-     1136167  Jan 22 2013 14:14:11 -08:00  system-report_1_20130122-221322-UTC.gz
34821  -rw-     1094631   Jan 2 2013 17:59:23 -08:00  system-report_1_20130103-015835-UTC.gz

 6147  -rw-      967429   Jan 3 2013 10:32:44 -08:00  system-report_1_20130103-183156-UTC.gz
34824  -rwx          50  Jan 22 2013 14:14:14 -08:00  deleted_sysreport_files
6155  -rwx         373  Jan 22 2013 14:14:13 -08:00  last_systemreport_log

145898496 bytes total (18569216 bytes free)
stack3#

The file name of the most recent crashinfo file is stored in last_crashinfo.
The file name of the most recent system report is stored in last_systemreport.


Switch#
```

System Reports

When a switch crashes, a system report is automatically generated for each switch in the switch stack. The system report file captures all the trace buffers, and other system-wide logs found on the switch. System reports are located in the crashinfo directory in the following format:

```
system-report_[switch number]_[date]-[timestamp]-UTC.gz
```

After a switch crash, you should check if a system report file was generated. The name of the most recently generated system report file is stored in the last_systemreport file under the crashinfo directory. The system report and crashinfo files assist TAC when troubleshooting your issue.

Onboard Failure Logging on the Switch

You can use the onboard failure logging (OBFL) feature to collect information about the Switch. The information includes uptime, temperature, and voltage information and helps Cisco technical support representatives to troubleshoot Switch problems. We recommend that you keep OBFL enabled and do not erase the data stored in the flash memory.

By default, OBFL is enabled. It collects information about the Switch and small form-factor pluggable (SFP) modules. The Switch stores this information in the flash memory:

- CLI commands—Record of the OBFL CLI commands that are entered on a standalone Switch or a switch stack member.
- Environment data—Unique device identifier (UDI) information for a standalone Switch or a switch stack member and for all the connected FRU devices: the product identification (PID), the version identification (VID), and the serial number.
- Message—Record of the hardware-related system messages generated by a standalone Switch or a switch stack member.
- Power over Ethernet (PoE)—Record of the power consumption of PoE ports on a standalone Switch or a switch stack member.
- Temperature—Temperature of a standalone Switch or a switch stack member.
- Uptime data—Time when a standalone Switch or a switch stack member starts, the reason the Switch restarts, and the length of time the Switch has been running since it last restarted.
- Voltage—System voltages of a standalone Switch or a switch stack member.

You should manually set the system clock or configure it by using Network Time Protocol (NTP).

When the Switch is running, you can retrieve the OBFL data by using the **show logging onboard** privileged EXEC commands. If the Switch fails, contact your Cisco technical support representative to find out how to retrieve the data.

When an OBFL-enabled Switch is restarted, there is a 10-minute delay before logging of new data begins.

Related Topics

Configuring OBFL, on page 1424
Displaying OBFL Information, on page 1426

Fan Failures

By default, the feature is disabled. When more than one of the fans fails in a field-replaceable unit (FRU) or in a power supply, the Switch does not shut down, and this error message appears:

```
Multiple fan(FRU/PS) failure detected. System may get overheated. Change fan quickly.
```

The Switch might overheat and shut down.

To enable the fan failures feature, enter the **system env fan-fail-action shut** privileged EXEC command. If more than one fan in the Switch fails, the Switch automatically shuts down, and this error message appears:

```
Faulty (FRU/PS) fans detected, shutting down system!
```

After the first fan shuts down, if the Switch detects a second fan failure, the Switch waits for 20 seconds before it shuts down.

To restart the Switch, it must be power cycled.

Possible Symptoms of High CPU Utilization

Excessive CPU utilization might result in these symptoms, but the symptoms might also result from other causes:

Note You may see increased system memory usage when Cisco Catalyst 4500E Supervisor Engine 8-E is used in wireless mode.

- Spanning tree topology changes
- EtherChannel links brought down due to loss of communication
- Failure to respond to management requests (ICMP ping, SNMP timeouts, slow Telnet or SSH sessions)
- UDLD flapping
- IP SLAs failures because of SLAs responses beyond an acceptable threshold
- DHCP or IEEE 802.1x failures if the switch does not forward or respond to requests

How to Troubleshoot the Software Configuration

Recovering from a Software Failure

Before you begin

This recovery procedure requires that you have physical access to the switch.

This procedure uses boot loader commands and TFTP to recover from a corrupted or incorrect image file.

Procedure

Step 1 From your PC, download the software image file (*image.bin*) from Cisco.com.

Step 2 Load the software image to your TFTP server.

Step 3 Connect your PC to the switch Ethernet management port.

Step 4 Unplug the switch power cord.

Step 5 Press the **Mode** button, and at the same time, reconnect the power cord to the switch.

Step 6 From the bootloader (ROMMON) prompt, ensure that you can ping your TFTP server.

a) Set the IP address **switch: set IP_ADDRESS** *ip_address subnet_mask*

Example:

```
switch: set IP_ADDRESS 192.0.2.123/255.255.255.0
```

b) Set the default router IP address **switch: set DEFAULT_ROUTER** *ip_address*

Example:

```
switch: set DEFAULT_ROUTER 192.0.2.1
```

c) Verify that you can ping the TFTP server **switch: ping** *ip_address_of_TFTP_server*

Example:

```
switch: ping 192.0.2.15
ping 192.0.2.1 with 32 bytes of data...
Host 192.0.2.1 is alive.
switch:
```

Step 7 Verify that you have a recovery image in your recovery partition (sda9:).

This recovery image is required for recovery using the emergency-install feature.

Example:

```
switch: dir sda9:
Directory of sda9:/

    2  drwx  1024       .
    2  drwx  1024       ..
   11  -rw-  18923068   c3850-recovery.bin

36939776 bytes available (20830208 bytes used)
switch:
```

Step 8 From the bootloader (ROMMON) prompt, initiate the emergency-install feature that assists you in recovering the software image on your switch.

WARNING: The emergency install command will erase your entire boot flash!

Example:

```
Switch#
emergency-install
tftp://192.0.2.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin

The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery
(tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin)...
Reading full image into memory.....................done
Nova Bundle Image
--------------------------------------
Kernel Address : 0x6042e5cc
Kernel Size : 0x318261/3244641
Initramfs Address : 0x60746830
Initramfs Size : 0xdb0fb9/14356409
Compression Format: .mzip
```

```
Bootable image at @ ram:0x6042e5cc
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000,
0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "sda9:c3850-recovery.bin" uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)



Initiating Emergency Installation of bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin


Downloading bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Validating bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Installing bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Verifying bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Package cat3k_caa-base..pkg is Digitally Signed
Package cat3k_caa-drivers.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-infra.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-iosd-universalk9.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-platform.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-wcm.SPA.03.02.00.SE.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.



Booting...(use DDR clock 667 MHz)Initializing and Testing RAM +++@@@@####...++@@++@@++@@++@
```

Related Topics

Software Failure on a Switch, on page 1405

Recovering from a Lost or Forgotten Password

The default configuration for the switch allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process during power-on and by entering a new password. These recovery procedures require that you have physical access to the switch.

Note On these switches, a system administrator can disable some of the functionality of this feature by allowing an end user to reset a password only by agreeing to return to the default configuration. If you are an end user trying to reset a password when password recovery has been disabled, a status message shows this during the recovery process.

Procedure

Step 1 Connect a terminal or PC to the switch.

- Connect a terminal or a PC with terminal-emulation software to the switch console port.
- Connect a PC to the Ethernet management port.

Step 2 Set the line speed on the emulation software to 9600 baud.

Step 3 Power off the standalone switch or the entire switch stack.

Step 4 Reconnect the power cord to the or the . Within 15 seconds, press the **Mode** button while the System LED is still flashing green. Continue pressing the **Mode** button until a prompt is seen; then release the **Mode** button.

```
Switch:
Xmodem file system is available.
Base ethernet MAC Address: 20:37:06:4d:e9:80
Verifying bootloader digital signature.


The system has been interrupted prior to loading the operating
system software, console will be reset to 9600 baud rate.
```

Proceed to the *Procedure with Password Recovery Enabled* section, and follow the steps.

Step 5 After recovering the password, reload the switch or the .

On a switch:

```
Switch> reload
Proceed with reload? [confirm] y
```

Related Topics

Lost or Forgotten Password on a Switch, on page 1406

Procedure with Password Recovery Enabled

If the password-recovery operation is enabled, this message appears:

Procedure

Step 1 Initialize the flash file system.

```
Switch: flash_init
```

Step 2 Ignore the startup configuration with the following command:

```
Switch: SWITCH_IGNORE_STARTUP_CFG=1
```

Step 3 Boot the switch with the *packages.conf* file from flash.

```
Switch: boot flash:packages.conf
```

Step 4 Terminate the initial configuration dialog by answering **No**.

```
Would you like to enter the initial configuration dialog? [yes/no]: No
```

Step 5 At the switch prompt, enter privileged EXEC mode.

```
Switch> enable
Switch#
```

Step 6 Copy the startup configuration to running configuration.

```
Switch# copy startup-config running-config Destination filename [running-config]?
```

Press Return in response to the confirmation prompts. The configuration file is now reloaded, and you can change the password.

Step 7 Enter global configuration mode and change the **enable** password.

```
Switch# configure terminal
Switch(config)#
```

Step 8 Write the running configuration to the startup configuration file.

```
Switch(config)# copy running-config startup-config
```

Step 9 Confirm that manual boot mode is enabled.

```
Switch# show boot

 BOOT variable = flash:packages.conf;
 Manual Boot = yes
 Enable Break = yes
```

Step 10 Reload the switch.

```
Switch# reload
```

Step 11 Return the Bootloader parameters (previously changed in Steps 2 and 3) to their original values.

```
switch: SWITCH_IGNORE_STARTUP_CFG=0
```

Step 12 Boot the switch with the *packages.conf* file from flash.

```
Switch: boot flash:packages.conf
```

Step 13 After the switch boots up, disable manual boot on the switch.

```
Switch(config)# no boot manual
```

Procedure with Password Recovery Disabled

If the password-recovery mechanism is disabled, this message appears:

```
The password-recovery mechanism has been triggered, but
is currently disabled.  Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point.  However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default configuration (y/n)?
```

Caution Returning the Switch to the default configuration results in the loss of all existing configurations. We recommend that you contact your system administrator to verify if there are backup Switch and VLAN configuration files.

- If you enter **n** (no), the normal boot process continues as if the **Mode** button had not been pressed; you cannot access the boot loader prompt, and you cannot enter a new password. You see the message:

  ```
  Press Enter to continue........
  ```

- If you enter **y** (yes), the configuration file in flash memory and the VLAN database file are deleted. When the default configuration loads, you can reset the password.

Procedure

Step 1 Choose to continue with password recovery and delete the existing configuration:

```
Would you like to reset the system back to the default configuration (y/n)? Y
```

Step 2 Display the contents of flash memory:

```
Switch: dir flash:
```

The Switch file system appears.

```
Directory of flash:/
.
.
.i'
15494  drwx        4096   Jan 1 2000 00:20:20 +00:00  kirch
15508  -rw-   258065648   Sep 4 2013 14:19:03 +00:00
cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
162196684
```

Step 3 Boot up the system:

```
Switch: boot
```

You are prompted to start the setup program. To continue with password recovery, enter **N** at the prompt:

```
Continue with the configuration dialog? [yes/no]: N
```

Step 4 At the Switch prompt, enter privileged EXEC mode:

```
Switch> enable
```

Step 5 Enter global configuration mode:

```
Switch# configure terminal
```

Step 6 Change the password:

```
Switch(config)# enable secret password
```

The secret password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, and allows spaces but ignores leading spaces.

Step 7 Return to privileged EXEC mode:

```
Switch(config)# exit
Switch#
```

Note Before continuing to Step 9, power on any connected stack members and wait until they have completely initialized.

Step 8 Write the running configuration to the startup configuration file:

```
Switch# copy running-config startup-config
```

The new password is now in the startup configuration.

Step 9 You must now reconfigure the Switch. If the system administrator has the backup Switch and VLAN configuration files available, you should use those.

Preventing Switch Stack Problems

To prevent switch stack problems, you should do the following:

- Make sure that the Switch that you add to or remove from the switch stack are powered off. For all powering considerations in switch stacks, see the "Switch Installation" chapter in the hardware installation guide.
- Press the **Mode** button on a stack member until the Stack mode LED is on. The last two port LEDs on the Switch should be green. Depending on the Switch model, the last two ports are either 10/100/1000 ports or small form-factor pluggable (SFP) module. If one or both of the last two port LEDs are not green, the stack is not operating at full bandwidth.
- We recommend using only one CLI session when managing the switch stack. Be careful when using multiple CLI sessions to the . Commands that you enter in one session are not displayed in the other sessions. Therefore, it is possible that you might not be able to identify the session from which you entered a command.
- Manually assigning stack member numbers according to the placement of the Switch in the stack can make it easier to remotely troubleshoot the switch stack. However, you need to remember that the Switch have manually assigned numbers if you add, remove, or rearrange Switch later. Use the **switch** *current-stack-member-number* **renumber** *new-stack-member-number* global configuration command to manually assign a stack member number.

If you replace a stack member with an identical model, the new Switch functions with the exact same configuration as the replaced Switch. This is also assuming the new Switch is using the same member number as the replaced Switch.

Removing powered-on stack members causes the switch stack to divide (partition) into two or more switch stacks, each with the same configuration. If you want the switch stacks to remain separate, change the IP address or addresses of the newly created switch stacks. To recover from a partitioned switch stack, follow these steps:

1. Power off the newly created switch stacks.
2. Reconnect them to the original switch stack through their StackWise Plus ports.
3. Power on the Switch.

For the commands that you can use to monitor the switch stack and its members, see the *Displaying Switch Stack Information* section.

Preventing Autonegotiation Mismatches

The IEEE 802.3ab autonegotiation protocol manages the Switch settings for speed (10 Mb/s, 100 Mb/s, and 1000 Mb/s, excluding SFP module ports) and duplex (half or full). There are situations when this protocol can incorrectly align these settings, reducing performance. A mismatch occurs under these circumstances:

- A manually set speed or duplex parameter is different from the manually set speed or duplex parameter on the connected port.
- A port is set to autonegotiate, and the connected port is set to full duplex with no autonegotiation.

To maximize Switch performance and ensure a link, follow one of these guidelines when changing the settings for duplex and speed:

- Let both ports autonegotiate both speed and duplex.
- Manually set the speed and duplex parameters for the ports on both ends of the connection.

Note If a remote device does not autonegotiate, configure the duplex settings on the two ports to match. The speed parameter can adjust itself even if the connected port does not autonegotiate.

Troubleshooting SFP Module Security and Identification

Cisco small form-factor pluggable (SFP) modules have a serial EEPROM that contains the module serial number, the vendor name and ID, a unique security code, and cyclic redundancy check (CRC). When an SFP module is inserted in the Switch, the Switch software reads the EEPROM to verify the serial number, vendor name and vendor ID, and recompute the security code and CRC. If the serial number, the vendor name or vendor ID, the security code, or CRC is invalid, the software generates a security error message and places the interface in an error-disabled state.

Note The security error message references the GBIC_SECURITY facility. The Switch supports SFP modules and does not support GBIC modules. Although the error message text refers to GBIC interfaces and modules, the security messages actually refer to the SFP modules and module interfaces.

If you are using a non-Cisco SFP module, remove the SFP module from the Switch, and replace it with a Cisco module. After inserting a Cisco SFP module, use the **errdisable recovery cause gbic-invalid** global configuration command to verify the port status, and enter a time interval for recovering from the error-disabled state. After the elapsed interval, the Switch brings the interface out of the error-disabled state and retries the operation. For more information about the **errdisable recovery** command, see the command reference for this release.

If the module is identified as a Cisco SFP module, but the system is unable to read vendor-data information to verify its accuracy, an SFP module error message is generated. In this case, you should remove and reinsert the SFP module. If it continues to fail, the SFP module might be defective.

Monitoring SFP Module Status

You can check the physical or operational status of an SFP module by using the **show interfaces transceiver** privileged EXEC command. This command shows the operational status, such as the temperature and the current for an SFP module on a specific interface and the alarm status. You can also use the command to check the speed and the duplex settings on an SFP module. For more information, see the **show interfaces transceiver** command in the command reference for this release.

Executing Ping

If you attempt to ping a host in a different IP subnetwork, you must define a static route to the network or have IP routing configured to route between those subnets.

IP routing is disabled by default on all Switch.

Note Though other protocol keywords are available with the **ping** command, they are not supported in this release.

Use this command to ping another device on the network from the Switch:

Command	Purpose
ping ip *host* | *address* `Switch# ping 172.20.52.3`	Pings a remote host through IP or by supplying the hostname or network address.

Related Topics

Ping, on page 1407
Example: Pinging an IP Host, on page 1430

Monitoring Temperature

The Switch monitors the temperature conditions and uses the temperature information to control the fans.

Use the **show env temperature status** privileged EXEC command to display the temperature value, state, and thresholds. The temperature value is the temperature in the Switch (not the external temperature).You can configure only the yellow threshold level (in Celsius) by using the **system env temperature threshold yellow** *value* global configuration command to set the difference between the yellow and red thresholds. You cannot configure the green or red thresholds. For more information, see the command reference for this release.

Monitoring the Physical Path

You can monitor the physical path that a packet takes from a source device to a destination device by using one of these privileged EXEC commands:

Table 110: Monitoring the Physical Path

Command	Purpose
tracetroute mac [**interface** *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]	Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.
tracetroute mac ip {*source-ip-address* | *source-hostname*} {*destination-ip-address* | *destination-hostname*} [**detail**]	Displays the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

Executing IP Traceroute

Note Though other protocol keywords are available with the **traceroute** privileged EXEC command, they are not supported in this release.

Command	Purpose
traceroute ip *host* `Switch# traceroute ip 192.51.100.1`	Traces the path that packets take through the network.

Related Topics

IP Traceroute , on page 1408
Example: Performing a Traceroute to an IP Host, on page 1431

Running TDR and Displaying the Results

To run TDR, enter the **test cable-diagnostics tdr interface** *interface-id* privileged EXEC command.

To display the results, enter the **show cable-diagnostics tdr interface** *interface-id* privileged EXEC command.

Redirecting Debug and Error Message Output

By default, the network server sends the output from **debug** commands and system error messages to the console. If you use this default, you can use a virtual terminal connection to monitor debug output instead of connecting to the console port or the Ethernet management port.

Possible destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. The syslog format is compatible with 4.3 Berkeley Standard Distribution (BSD) UNIX and its derivatives.

Note Be aware that the debugging destination you use affects system overhead. When you log messages to the console, very high overhead occurs. When you log messages to a virtual terminal, less overhead occurs. Logging messages to a syslog server produces even less, and logging to an internal buffer produces the least overhead of any method.

For more information about system message logging, see *Configuring System Message Logging*.

Related Topics

Debug Commands, on page 1410

Using the show platform forward Command

The output from the **show platform forward** privileged EXEC command provides some useful information about the forwarding results if a packet entering an interface is sent through the system. Depending upon the parameters entered about the packet, the output provides lookup table results and port maps used to calculate forwarding destinations, bitmaps, and egress information.

Most of the information in the output from the command is useful mainly for technical support personnel, who have access to detailed information about the Switch application-specific integrated circuits (ASICs). However, packet forwarding information can also be helpful in troubleshooting.

Using the show debug command

The **show debug** command is entered in privileged EXEC mode. This command displays all debug options available on the switch.

To view all conditional debug options run the command **show debug condition** The commands can be listed by selecting either a condition identifier *<1-1000>* or *all* conditions.

To disable debugging, use the **no debug all** command.

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

For more information, see *Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 16.1 (Catalyst 3850 Switches)*.

Configuring OBFL

Caution We recommend that you do not disable OBFL and that you do not remove the data stored in the flash memory.

- To enable OBFL, use the **hw-switch switch** [*switch-number*] **logging onboard** [**message level** *level*] global configuration command. On switches, the range for *switch-number* is from 1 to 9. Use the **message level** *level* parameter to specify the severity of the hardware-related messages that the switch generates and stores in the flash memory.
- To copy the OBFL data to the local network or a specific file system, use the **copy onboard switch** *switch-number* **url** *url-destination* privileged EXEC command.
- To disable OBFL, use the **no hw-switch switch** [*switch-number*] **logging onboard** [**message level**] global configuration command.
- To clear all the OBFL data in the flash memory except for the uptime and CLI command information, use the **clear onboard switch** *switch-number* privileged EXEC command.
- In a switch stack, you can enable OBFL on a standalone switch or on all stack members by using the **hw-switch switch** [*switch-number*] **logging onboard** [**message level** *level*] global configuration command.
- You can enable or disable OBFL on a member switch from the .

For more information about the commands in this section, see the command reference for this release.

Related Topics

Onboard Failure Logging on the Switch, on page 1412
Displaying OBFL Information, on page 1426

WSMA Configuration for WebUI

WSMA configurations are available by default to access the Web UI. If you explicitly delete the configuration, you have to reconfigure as below:

```
Switch(config)#wsma agent exec
Switch(wsma-exec-agent)# profile httplistener
Switch(wsma-exec-agent)# profile httpslistener
Switch(wsma-exec-agent)#exit
Switch(config)#wsma agent config
Switch(wsma-config-agent)# profile httplistener
Switch(wsma-config-agent)# profile httpslistener
Switch(wsma-config-agent)#exit
Switch(config)#wsma agent filesys
Switch(wsma-filesys-agent)# profile httplistener
Switch(wsma-filesys-agent)# profile httpslistener
Switch(wsma-filesys-agent)#exit
Switch(config)#wsma agent notify
```

Verifying Troubleshooting of the Software Configuration

Displaying OBFL Information

Table 111: Commands for Displaying OBFL Information

Command	Purpose
show onboard switch *switch-number* **clilog** `Switch# show onboard switch 1 clilog`	Displays the OBFL CLI commands that were entered on a standalone switch or the specified stack members.
show onboard switch *switch-number* **environment** `Switch# show onboard switch 1 environment`	Displays the UDI information for a standalone switch or the specified stack members and for all the connected FRU devices: the PID, the VID, and the serial number.
show onboard switch *switch-number* **message** `Switch# show onboard switch 1 message`	Displays the hardware-related messages generated by a standalone switch or the specified stack members.
show onboard switch *switch-number* **counter** `Switch# show onboard switch 1 counter`	Displays the counter information on a standalone switch or the specified stack members.
show onboard switch *switch-number* **temperature** `Switch# show onboard switch 1 temperature`	Displays the temperature of a standalone switch or the specified switch stack members.
show onboard switch *switch-number* **uptime** `Switch# show onboard switch 1 uptime`	Displays the time when a standalone switch or the specified stack members start, the reason the standalone switch or specified stack members restart, and the length of time that the standalone switch or specified stack members have been running since they last restarted.
show onboard switch *switch-number* **voltage** `Switch# show onboard switch 1 voltage`	Displays the system voltages of a standalone switch or the specified stack members.
show onboard switch *switch-number* **status** `Switch# show onboard switch 1 status`	Displays the status of a standalone switch or the specified stack members.

Related Topics

Onboard Failure Logging on the Switch, on page 1412
Configuring OBFL, on page 1424

Example: Verifying the Problem and Cause for High CPU Utilization

To determine if high CPU utilization is a problem, enter the **show processes cpu sorted** privileged EXEC command. Note the underlined information in the first line of the output example.

```
Switch# show processes cpu sorted
CPU utilization for five seconds: 8%/0%; one minute: 7%; five minutes: 8%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
309 42289103 752750 56180 1.75% 1.20% 1.22% 0 RIP Timers
140 8820183 4942081 1784 0.63% 0.37% 0.30% 0 HRPC qos request
100 3427318 16150534 212 0.47% 0.14% 0.11% 0 HRPC pm-counters
192 3093252 14081112 219 0.31% 0.14% 0.11% 0 Spanning Tree
143 8 37 216 0.15% 0.01% 0.00% 0 Exec
...
<output truncated>
```

This example shows normal CPU utilization. The output shows that utilization for the last 5 seconds is 8%/0%, which has this meaning:

- The total CPU utilization is 8 percent, including both time running Cisco IOS processes and time spent handling interrupts.
- The time spent handling interrupts is zero percent.

Table 112: Troubleshooting CPU Utilization Problems

Type of Problem	Cause	Corrective Action
Interrupt percentage value is almost as high as total CPU utilization value.	The CPU is receiving too many packets from the network.	Determine the source of the network packet. Stop the flow, or change the switch configuration. See the section on "Analyzing Network Traffic."
Total CPU utilization is greater than 50% with minimal time spent on interrupts.	One or more Cisco IOS process is consuming too much CPU time. This is usually triggered by an event that activated the process.	Identify the unusual event, and troubleshoot the root cause. See the section on "Debugging Active Processes."

Scenarios for Troubleshooting the Software Configuration

Scenarios to Troubleshoot Power over Ethernet (PoE)

Table 113: Power over Ethernet Troubleshooting Scenarios

Symptom or Problem	Possible Cause and Solution
Only one port does not have PoE. Trouble is on only one switch port. PoE and non-PoE devices do not work on this port, but do on other ports.	Verify that the powered device works on another PoE port. Use the **show run**, or **show interface status** user EXEC commands to verify that the port is not shut down or error-disabled. **Note** Most switches turn off port power when the port is shut down, even though the IEEE specifications make this optional. Verify that **power inline never** is not configured on that interface or port. Verify that the Ethernet cable from the powered device to the switch port is good: Connect a known good non-PoE Ethernet device to the Ethernet cable, and make sure that the powered device establishes a link and exchanges traffic with another host. **Note** Cisco powered device works only with straight cable and not with crossover one. Verify that the total cable length from the switch front panel to the powered device is not more than 100 meters. Disconnect the Ethernet cable from the switch port. Use a short Ethernet cable to connect a known good Ethernet device directly to this port on the switch front panel (not on a patch panel). Verify that it can establish an Ethernet link and exchange traffic with another host, or ping the port VLAN SVI. Next, connect a powered device to this port, and verify that it powers on. If a powered device does not power on when connected with a patch cord to the switch port, compare the total number of connected powered devices to the switch power budget (available PoE). Use the **show inline power** command to verify the amount of available power.

Symptom or Problem	Possible Cause and Solution
No PoE on all ports or a group of ports. Trouble is on all switch ports. Nonpowered Ethernet devices cannot establish an Ethernet link on any port, and PoE devices do not power on.	If there is a continuous, intermittent, or reoccurring alarm related to power, replace the power supply if possible it is a field-replaceable unit. Otherwise, replace the switch. If the problem is on a consecutive group of ports but not all ports, the power supply is probably not defective, and the problem could be related to PoE regulators in the switch. Use the **show log** privileged EXEC command to review alarms or system messages that previously reported PoE conditions or status changes. If there are no alarms, use the **show interface status** command to verify that the ports are not shut down or error-disabled. If ports are error-disabled, use the **shut** and **no shut** interface configuration commands to reenable the ports. Use the **show env power** and **show power inline** privileged EXEC commands to review the PoE status and power budget (available PoE). Review the running configuration to verify that **power inline never** is not configured on the ports. Connect a nonpowered Ethernet device directly to a switch port. Use only a short patch cord. Do not use the existing distribution cables. Enter the **shut** and **no shut** interface configuration commands, and verify that an Ethernet link is established. If this connection is good, use a short patch cord to connect a powered device to this port and verify that it powers on. If the device powers on, verify that all intermediate patch panels are correctly connected. Disconnect all but one of the Ethernet cables from switch ports. Using a short patch cord, connect a powered device to only one PoE port. Verify the powered device does not require more power than can be delivered by the switch port. Use the **show power inline** privileged EXEC command to verify that the powered device can receive power when the port is not shut down. Alternatively, watch the powered device to verify that it powers on. If a powered device can power on when only one powered device is connected to the switch, enter the **shut** and **no shut** interface configuration commands on the remaining ports, and then reconnect the Ethernet cables one at a time to the switch PoE ports. Use the **show interface status** and **show power inline** privileged EXEC commands to monitor inline power statistics and port status. If there is still no PoE at any port, a fuse might be open in the PoE section of the power supply. This normally produces an alarm. Check the log again for alarms reported earlier by system messages.

Symptom or Problem	Possible Cause and Solution
Cisco pre-standard powered device disconnects or resets. After working normally, a Cisco phone intermittently reloads or disconnects from PoE.	Verify all electrical connections from the switch to the powered device. Any unreliable connection results in power interruptions and irregular powered device functioning such as erratic powered device disconnects and reloads. Verify that the cable length is not more than 100 meters from the switch port to the powered device. Notice what changes in the electrical environment at the switch location or what happens at the powered device when the disconnect occurs. Notice whether any error messages appear at the same time a disconnect occurs. Use the **show log** privileged EXEC command to review error messages. Verify that an IP phone is not losing access to the Call Manager immediately before the reload occurs. (It might be a network problem and not a PoE problem.) Replace the powered device with a non-PoE device, and verify that the device works correctly. If a non-PoE device has link problems or a high error rate, the problem might be an unreliable cable connection between the switch port and the powered device.
IEEE 802.3af-compliant or IEEE 802.3at-compliant powered devices do not work on Cisco PoE switch. A non-Cisco powered device is connected to a Cisco PoE switch, but never powers on or powers on and then quickly powers off. Non-PoE devices work normally.	Use the **show power inline** command to verify that the switch power budget (available PoE) is not depleted before or after the powered device is connected. Verify that sufficient power is available for the powered device type before you connect it. Use the **show interface status** command to verify that the switch detects the connected powered device. Use the **show log** command to review system messages that reported an overcurrent condition on the port. Identify the symptom precisely: Does the powered device initially power on, but then disconnect? If so, the problem might be an initial surge-in (or *inrush*) current that exceeds a current-limit threshold for the port.

Related Topics

Power over Ethernet Ports, on page 1406

Configuration Examples for Troubleshooting Software

Example: Pinging an IP Host

This example shows how to ping an IP host:

```
Switch# ping 172.20.52.3
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Switch#
```

Table 114: Ping Output Display Characters

Character	Description
!	Each exclamation point means receipt of a reply.
.	Each period means the network server timed out while waiting for a reply.
U	A destination unreachable error PDU was received.
C	A congestion experienced packet was received.
I	User interrupted test.
?	Unknown packet type.
&	Packet lifetime exceeded.

To end a ping session, enter the escape sequence (**Ctrl-^ X** by default). Simultaneously press and release the **Ctrl**, **Shift**, and **6** keys and then press the **X** key.

Related Topics

Ping, on page 1407
Executing Ping, on page 1422

Example: Performing a Traceroute to an IP Host

This example shows how to perform a **traceroute** to an IP host:

```
Switch# traceroute ip 192.0.2.10

Type escape sequence to abort.
Tracing the route to 192.0.2.10

  1 192.0.2.1 0 msec 0 msec 4 msec
  2 192.0.2.203 12 msec 8 msec 0 msec
  3 192.0.2.100 4 msec 0 msec 0 msec
  4 192.0.2.10 0 msec 4 msec 0 msec
```

The display shows the hop count, the IP address of the router, and the round-trip time in milliseconds for each of the three probes that are sent.

Table 115: Traceroute Output Display Characters

Character	Description
*	The probe timed out.
?	Unknown packet type.

Character	Description
A	Administratively unreachable. Usually, this output means that an access list is blocking traffic.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
U	Port unreachable.

To end a trace in progress, enter the escape sequence (**Ctrl-^ X** by default). Simultaneously press and release the **Ctrl**, **Shift**, and **6** keys and then press the **X** key.

Related Topics

IP Traceroute , on page 1408
Executing IP Traceroute, on page 1423

Example: Enabling All System Diagnostics

Caution Because debugging output takes priority over other network traffic, and because the **debug all** privileged EXEC command generates more output than any other **debug** command, it can severely diminish switch performance or even render it unusable. In virtually all cases, it is best to use more specific **debug** commands.

This command disables all-system diagnostics:

```
Switch# debug all
```

The **no debug all** privileged EXEC command disables all diagnostic output. Using the **no debug all** command is a convenient way to ensure that you have not accidentally left any **debug** commands enabled.

Related Topics

Debug Commands, on page 1410

Additional References for Troubleshooting Software Configuration

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference (Catalyst 3850 Switches)System Management Command Reference (Cisco WLC 5700 Series)*
Platform-independent command reference	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*
Platform_independent configuration information	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for Troubleshooting Software Configuration

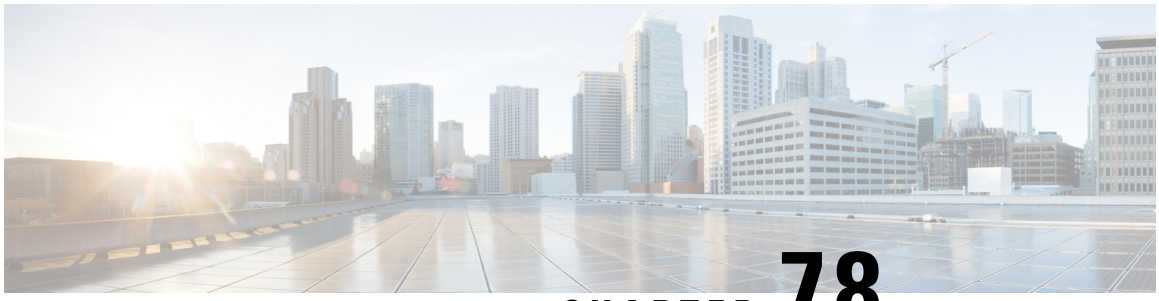
Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.

Related Topics

Finding Feature Information, on page 135

PART XIII

VideoStream



CHAPTER 78

Configuring VideoStream

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VideoStream

Make sure that the multicast feature is enabled. We recommend configuring IP multicast on the controller with multicast-multicast mode.

Check for the IP address on the client machine. The machine should have an IP address from the respective VLAN.

Verify that the access points have joined the controllers.

Restrictions for Configuring VideoStream

IGMP snooping is required to switch ON for this MC2UC feature to be functional.

Cisco 5700 Series WLC is not supported in centralized cmm mode.

Information about VideoStream

The IEEE 802.11 wireless multicast delivery mechanism does not provide a reliable way to acknowledge lost or corrupted packets. The multicast frame packets are sent at a predetermined rate irrespective of the wireless client optimal data rate. As a result, if any multicast packet is lost in the air, it is not sent again which may cause an IP multicast stream unviewable. Also if the packets are delivered faster, the packets get congested.

The VideoStream feature makes the IP multicast stream delivery reliable over the air, by converting the multicast frame to a unicast frame over the air. Each VideoStream client acknowledges receiving a video IP multicast stream.

How to Configure VideoStream

Configuring Multicast-Direct Globally for Media-Stream

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wireless multicast** **Example:**	Enables multicast for wireless forwarding.
Step 3	**IP igmp snooping** **Example:**	Enables IGMP snooping on a per-VLAN basis. If the global setting is disabled, then all VLANs are treated as disabled, whether they are enabled or not.
Step 4	**IP igmp snooping querier** **Example:**	Configures a snooping querier on an interface when there is no multicast router in the VLAN to generate queries.
Step 5	**wireless media-stream multicast-direct** **Example:** `Switch(config)#wireless media-stream multicast-direct`	Configures the global multicast-direct feature for the controller.

Step 6	**wireless media-stream message**
	Example:
	`Switch(config)#wireless media-stream message ?`
	`  Email  Configure Session Announcement Email`
	`  Notes  Configure Session Announcement`
		Configures various message configuration parameters like phone, URL, email and notes. That is, when a media stream is refused (due to bandwidth constraints), a message can be sent to the user. These parameters configure the messages to send IT support email address, notes (message to display explaining why the

	Command or Action	Purpose
	notes URL Configure Session Announcement URL phone Configure Session Announcement Phone number <cr>	stream was refused), URL to which the user can be redirected and the phone number that the user can call about the refused stream.

Step 7	**wireless media-stream group** *<name><startIp><endIp>*
	Example:
	`Switch(config)#wireless media-stream group grp1 231.1.1.1 239.1.1.3`
	`Switch(config-media-stream)#?`
	
	avg-packet-size Configures average packet size
	default Set a command to its defaults
	exit Exit sub-mode
	max-bandwidth Configures maximum Expected Stream Bandwidth in Kbps
	no Negate a command or set its defaults
	policy Configure media stream admission policy
	qos Configure Over the AIR QoS class, <'video'> ONLY
	
	<cr>
		Configures each media stream and its parameters like expected multicast destination addresses, stream bandwidth consumption and stream priority parameters.

Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Media-Stream for 802.11 bands

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz media-stream multicast-direct** **Example:** `Switch(config)#ap dot11 24ghz media-stream multicast-direct`	Configures if media stream (mc2uc) is allowed for 802.11 band
Step 3	**ap dot11 24ghz | 5ghz media-stream video-redirect**	Configures to redirect unicast video traffic to best effort queue.

	Command or Action	Purpose
	Example: `Switch(config)#ap dot11 24ghz media-stream video-redirect`	
Step 4	**ap dot11 24ghz | 5ghz media-stream multicast-direct admission-besteffort** **Example:** `Switch(config)#ap dot11 24ghz media-stream multicast-direct admission-besteffort`	Configures the media stream to still be sent through the best effort queue if a media stream cannot be prioritized due to bandwidth availability limitations. Add **no** in the command to drop the stream if the media stream cannot be prioritized due to bandwidth availability limitations.
Step 5	**ap dot11 24ghz | 5ghz media-stream multicast-direct client-maximum [<value >]** **Example:** `Switch(config)#ap dot11 24ghz media-stream multicast-direct client-max 15`	Configures maximum number of allowed media streams per individual client. The maximum is 15 and the default is 0. Value 0 denotes unlimited streams.
Step 6	**ap dot11 24ghz | 5ghz media-stream multicast-direct radio-maximum 20** **Example:**	Configures maximum number of radio streams. The range is from 1 to 20. Default is 0. Value 0 denotes unlimited streams.
Step 7	**ap dot11 24ghz | 5ghz cac multimedia max-bandwidth [<bandwidth>]** **Example:** `Switch(config)#ap dot11 24ghz cac multimedia max-bandwidth 60`	Configure maximum media (voice + video) bandwidth in %. The range is between 5% and 85%.
Step 8	**ap dot11 24ghz | 5ghz cac media-stream multicast-direct min_client_rate [<dot11_rate>]** **Example:** `Switch(config)#ap dot11 24ghz cac media-stream multicast-direct min_client_rate`	Configures the minimum PHY rate needed for a client to send media-stream as unicast. Clients communicating below this rate will not receive the media stream as a unicast flow. Typically, this PHY rate is equal to or higher than the rate at which multicast frames are sent.
Step 9	**ap dot11 5ghz cac media-stream**	Configures CAC parameters for media stream access category.
Step 10	**ap dot11 5ghz cac multimedia**	Configures CAC parameters for media access category, used for voice and video.
Step 11	**ap dot11 5ghz cac video**	Configures CAC parameters for video access category, used for voice signaling.
Step 12	**ap dot11 5ghz cac voice**	Configures CAC parameters for voice access category.

	Command or Action	Purpose
Step 13	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring WLAN to Stream Video

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan_name* **Example:** `Switch(config)#wlan wlan50`	Enters the WLAN configuration mode.
Step 3	**shutdown** **Example:** `Switch(config-wlan)#shutdown`	Disables the WLAN for configuring it parameters.
Step 4	**media-stream multicast-direct** **Example:** `Switch(config)#media-stream multicast-direct`	Configures the multicast-direct feature on media-stream for the WLAN.
Step 5	**no shutdown** **Example:** `Switch(config-wlan)#no shutdown`	Enables the WLAN.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Deleting a Media-Stream

Before you begin

The media-stream should be enabled and configured for it to be deleted.

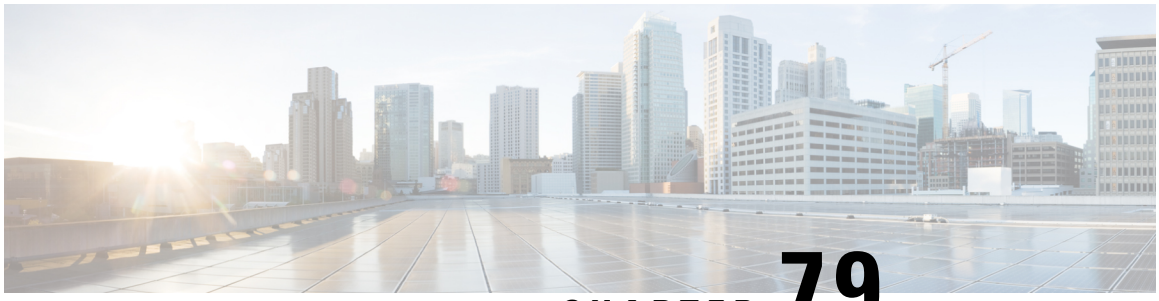
Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**no wireless media-stream group media_stream_name** **Example:** `Switch(config)#no wireless media-stream grp1`	Deletes the media-stream which bears the name mentioned in the command.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Monitoring Media Streams

Table 116: Commands for monitoring media streams

Commands	Description
show wireless media-stream client detail *group name*	Displays media stream client details of the particular group.
show wireless media-stream client summary	Displays the media stream information of all the clients.
show wireless media-stream group detail *group name*	Displays the media stream configuration details of the particular group.
show wireless media-stream group summary	Displays the media stream configuration details of all the groups.
show wireless media-stream message details	Displays the session announcement message details.
show wireless multicast	Displays the multicast-direct configuration state.
show ap dot11 24ghz | 5ghz media-stream rrc	Displays 802.11 media Resource-Reservation-Control configurations.



CHAPTER 79

Configuring VideoStream GUI

Configuring VideoStream (GUI)

Complete the following steps to configure VideoStream using GUI.

Procedure

Step 1 Configure the multicast feature by following these steps:

a) Choose **Wireless** > **MediaStream** > **General**.

b) Select or unselect the **Multicast Direct feature** check box. The default value is disabled.

Note Enabling the multicast direct feature does not automatically reset the existing client state. The wireless clients must rejoin the multicast stream after enabling the multicast direct feature on the controller.

c) In the **Session Message Config** area, select **Session announcement State** check box to enable the session announcement mechanism. If the session announcement state is enabled, clients are informed each time a controller is not able to serve the multicast direct data to the client.

d) In the **Session announcement URL** text box, enter the URL where the client can find more information when an error occurs during the multicast media stream transmission.

e) In the **Session announcement e-mail** text box, enter the e-mail address of the person who can be contacted.

f) In the **Session announcement Phone** text box, enter the phone number of the person who can be contacted.

g) In the **Session announcement Note** text box, enter a reason as to why a particular client cannot be served with a multicast media.

h) Click **Apply.**

Step 2 Add a media stream by following these steps:

a) Choose **Wireless** > **Media Stream** > **Streams** to open the Media Stream page.

b) Click **Add New** to configure a new media stream. The **Media Stream** > **New page** appears.

Note The Stream Name, Multicast Destination Start IP Address (IPv4 or IPv6), and Multicast Destination End IP Address (IPv4 or IPv6) text boxes are mandatory. You must enter information in these text boxes.

c) In the **Stream Name** text box, enter the media stream name. The stream name can be up to 64 characters.

d) In the **Multicast Destination Start IP Address (IPv4 or IPv6)** text box, enter the start (IPv4 or IPv6) address of the multicast media stream.

e) In the **Multicast Destination End IP Address (IPv4 or IPv6)** text box, enter the end (IPv4 or IPv6) address of the multicast media stream.

Example:

Note Ensure that the Multicast Destination Start and End IP addresses are of the same type, that is both addresses should be of either IPv4 or IPv6 type.

f) In the **Maximum Expected Bandwidth** text box, enter the maximum expected bandwidth that you want to assign to the media stream. The values can range between 1 to 35000 kbps.

Example:

Note We recommend that you use a template to add a media stream to the controller.

g) From the Select from Predefined Templates drop-down list under Resource Reservation Control (RRC) Parameters, choose one of the following options to specify the details about the resource reservation control:

- Very Coarse (below 300 kbps)
- Coarse (below 500 kbps)
- Ordinary (below 750 kbps)
- Low (below 1 Mbps)
- Medium (below 3 Mbps)
- High (below 5 Mbps)

Note When you select a predefined template from the drop-down list, the following text boxes under the Resource Reservation Control (RRC) Parameters list their default values that are assigned with the template.

- Average Packet Size (100-1500 bytes)—Specifies the average packet size. The value can be in the range of 100 to 1500 bytes. The default value is 1200.
- RRC Periodic update—Enables the RRC (Resource Reservation Control Check) Periodic update. By default, this option is enabled. RRC periodically updates the admission decision on the admitted stream according to the correct channel load. As a result, it may deny certain low priority admitted stream requests.
- RRC Priority (1-8)—Specifies the priority bit set in the media stream. The priority can be any number between 1 and 8. The larger the value means the higher the priority is. For example, a priority of 1 is the lowest value and a value of 8 is the highest value. The default priority is 4. The low priority stream may be denied in the RRC periodic update.
- Traffic Profile Violation—Specifies the action to perform in case of a violation after a re-RRC. Choose an action from the drop-down list. The possible values are as follows:

  Drop—Specifies that a stream is dropped on periodic revaluation.

  Fallback—Specifies that a stream is demoted to Best Effort class on periodic reevaluation.

  The default value is **drop**.

h) Click **Apply**.

Step 3 Enable the media stream for multicast-direct by following these steps:

a) Choose **WLANs** > **WLAN ID** to open the **WLANs** > **Edit** page.
b) Click the **QoS** tab and select Gold (Video) from the Quality of Service (QoS) drop-down list.
c) Click **Apply**.

Step 4 Set the EDCA parameters to voice and video optimized (optional) by following these steps:

a) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **EDCA** Parameters.
b) From the **EDCA Profile** drop-down list, choose the Voice and Video Optimized option.
c) Click **Apply**.

Step 5 Enable the admission control on a band for video (optional) by following these steps:

Note Keep the voice bandwidth allocation to a minimum for better performance.

a) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media** to open the 802.11a/n (5 GHZ) or 802.11b/g/n > Media page.
b) Click the **Video** tab.
c) Select the **Admission Control (ACM)** check box to enable bandwidth-based CAC for this radio band. The default value is disabled.
d) Click **Apply**

Step 6 Configure the video bandwidth by following these steps:

Note The template bandwidth that is configured for a media stream should be more than the bandwidth for the source media stream. The voice configuration is optional. Keep the voice bandwidth allocation to a minimum for better performance.

a) Disable all WMM WLANs.
b) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media** to open the 802.11a/n/ac (5 GHZ) or 802.11b/g/n > Media page.
c) Click the **Video** tab.
d) Select the **Admission Control (ACM)** check box to enable the video CAC for this radio band. The default value is disabled.
e) In the Max RF Bandwidth field, enter the percentage of the maximum bandwidth allocated to clients for video applications on this radio band. Once the client reaches the value specified, the access point rejects new requests on this radio band.

   The range is 5 to 85%. The default value is 9%.

f) Click **Apply**.
g) Reenable all WMM WLANs and click **Apply**.

Step 7 Configure the media bandwidth by following these steps:

a) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media** to open the 802.11a (or 802.11b) > Media > Parameters page.
b) Click the **Media** tab to open the Media page.
c) Select the **Unicast Video Redirect** check box to enable Unicast Video Redirect. The default value is disabled.
d) In the **Maximum Media Bandwidth (0-85%)** text box, enter the percentage of the maximum bandwidth to be allocated for media applications on this radio band. Once the client reaches a specified value, the access point rejects new calls on this radio band.

The default value is 85%; valid values are from 0% to 85%.

e) In the **Client Minimum Phy Rate** text box, enter the minimum transmission data rate to the client. If the transmission data rate is below the phy rate, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.

f) In the **Maximum Retry Percent (0-100%)** text box, enter the percentage of maximum retries that are allowed. The default value is 80. If it exceeds 80, either the video will not start or the client might be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.

g) Select the **Multicast Direct Enable** check box to enable the Multicast Direct Enable field. The default value is enabled.

h) From the **Max Streams per Radio** drop-down list, choose the maximum number of streams allowed per radio from the range 0 to 20. The default value is set to No-limit. If you choose No-limit, there is no limit set for the number of client subscriptions.

i) From the **Max Streams per Client** drop-down list, choose the maximum number of streams allowed per client from the range 0 to 20. The default value is set to No-limit. If you choose No-limit, there is no limit set for the number of client subscriptions.

j) Select the **Best Effort QoS Admission** check box to enable best-effort QoS admission.

k) Click **Apply**.

Step 8 Enable a WLAN by following these steps:

a) Choose **WLANS** > WLAN ID. The WLANs > Edit page appears.

b) Select the **Status** check box.

c) Click **Apply**.

Step 9 Enable the 802.11 a/n/ac or 802.11 b/g/n network by following these steps:

a) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Network**.

b) Select the **802.11a** or **802.11b/g Network Status** check box to enable the network status.

c) Click **Apply**.

Step 10 Verify that the clients are associated with the multicast groups and group IDs by following these steps:

a) Choose **Monitor** > **Clients**. The Clients page appears.

b) Check if the 802.11a/n/ac or 802.11b/g/n network clients have the associated access points.

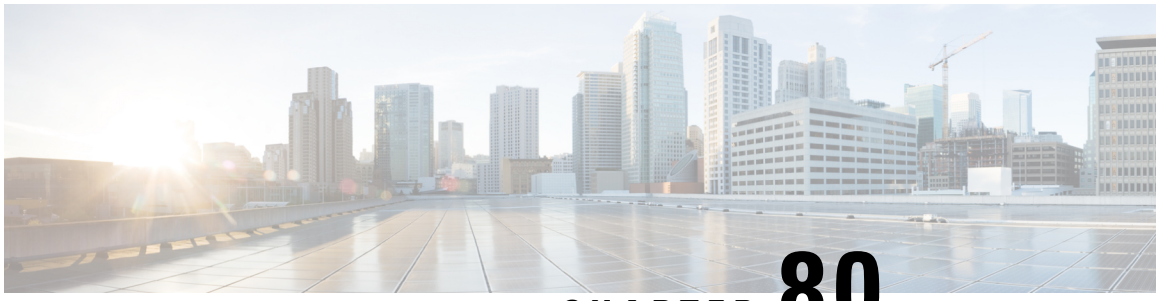
c) Choose **Monitor** > **Multicast**. The Multicast Groups page appears.

d) Select the **MGID** check box for the VideoStream to the clients.

e) Click **MGID**. The Multicast Group Detail page appears. Check the Multicast Status details.

PART XIV

VLAN



CHAPTER 80

Configuring VTP

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VTP

Before you create VLANs, you must decide whether to use the VLAN Trunking Protocol (VTP) in your network. Using VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network. Without VTP, you cannot send information about VLANs to other switches.

VTP is designed to work in an environment where updates are made on a single switch and are sent through VTP to other switches in the domain. It does not work well in a situation where multiple updates to the VLAN database occur simultaneously on switches in the same domain, which would result in an inconsistency in the VLAN database.

The switch supports a total of 4094 VLANs. However, the number of configured features affects the usage of the switch hardware. If the switch is notified by VTP of a new VLAN and the switch is already using the maximum available hardware resources, it sends a message that there are not enough hardware resources available and shuts down the VLAN. The output of the **show vlan** user EXEC command shows the VLAN in a suspended state.

Because trunk ports send and receive VTP advertisements, you must ensure that at least one trunk port is configured on the switch and that this trunk port is connected to the trunk port of another switch. Otherwise, the switch cannot receive any VTP advertisements.

Related Topics

VTP Advertisements, on page 1452
Adding a VTP Client Switch to a VTP Domain (CLI), on page 1466
VTP Domain, on page 1450
VTP Modes, on page 1451

Restrictions for VTP

The following are restrictions for a VTP:

- You cannot have a switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches.

⚠

Caution Before adding a VTP client switch to a VTP domain, always verify that its VTP configuration revision number is lower than the configuration revision number of the other switches in the VTP domain. Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number. If you add a switch that has a revision number higher than the revision number in the VTP domain, it can erase all VLAN information from the VTP server and VTP domain.

Information About VTP

VTP

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

VTP Domain

A VTP domain (also called a VLAN management domain) consists of one switch or several interconnected switches or switch stacks under the same administrative responsibility sharing the same VTP domain name. A switch can be in only one VTP domain. You make global VLAN configuration changes for the domain.

By default, the switch is in the VTP no-management-domain state until it receives an advertisement for a domain over a trunk link (a link that carries the traffic of multiple VLANs) or until you configure a domain

name. Until the management domain name is specified or learned, you cannot create or modify VLANs on a VTP server, and VLAN information is not propagated over the network.

If the switch receives a VTP advertisement over a trunk link, it inherits the management domain name and the VTP configuration revision number. The switch then ignores advertisements with a different domain name or an earlier configuration revision number.

When you make a change to the VLAN configuration on a VTP server, the change is propagated to all switches in the VTP domain. VTP advertisements are sent over all IEEE trunk connections, including IEEE 802.1Q. VTP dynamically maps VLANs with unique names and internal index associates across multiple LAN types. Mapping eliminates excessive device administration required from network administrators.

If you configure a switch for VTP transparent mode, you can create and modify VLANs, but the changes are not sent to other switches in the domain, and they affect only the individual switch. However, configuration changes made when the switch is in this mode are saved in the switch running configuration and can be saved to the switch startup configuration file.

Related Topics

Adding a VTP Client Switch to a VTP Domain (CLI), on page 1466
Prerequisites for VTP, on page 1449

VTP Modes

Table 117: VTP Modes

VTP Mode	Description
VTP server	In VTP server mode, you can create, modify, and delete VLANs, and specify other configuration parameters (such as the VTP version) for the entire VTP domain. VTP servers advertise their VLAN configurations to other switches in the same VTP domain and synchronize their VLAN configurations with other switches based on advertisements received over trunk links. VTP server is the default mode. In VTP server mode, VLAN configurations are saved in NVRAM. If the switch detects a failure while writing a configuration to NVRAM, VTP mode automatically changes from server mode to client mode. If this happens, the switch cannot be returned to VTP server mode until the NVRAM is functioning.

VTP Mode	Description
VTP client	A VTP client functions like a VTP server and transmits and receives VTP updates on its trunks, but you cannot create, change, or delete VLANs on a VTP client. VLANs are configured on another switch in the domain that is in server mode. In VTP versions 1 and 2 in VTP client mode, VLAN configurations are not saved in NVRAM. In VTP version 3, VLAN configurations are saved in NVRAM in client mode.
VTP transparent	VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2 or version 3, transparent switches do forward VTP advertisements that they receive from other switches through their trunk interfaces. You can create, modify, and delete VLANs on a switch in VTP transparent mode. When the switch is in VTP transparent mode, the VTP and VLAN configurations are saved in NVRAM, but they are not advertised to other switches. In this mode, VTP mode and domain name are saved in the switch running configuration, and you can save this information in the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command.
VTP off	A switch in VTP off mode functions in the same manner as a VTP transparent switch, except that it does not forward VTP advertisements on trunks.

Related Topics

Prerequisites for VTP, on page 1449
Configuring VTP Mode (CLI), on page 1458

VTP Advertisements

Each switch in the VTP domain sends periodic global configuration advertisements from each trunk port to a reserved multicast address. Neighboring switches receive these advertisements and update their VTP and VLAN configurations as necessary.

VTP advertisements distribute this global domain information:

- VTP domain name
- VTP configuration revision number

- Update identity and update timestamp
- MD5 digest VLAN configuration, including maximum transmission unit (MTU) size for each VLAN
- Frame format

VTP advertisements distribute this VLAN information for each configured VLAN:

- VLAN IDs (including IEEE 802.1Q)
- VLAN name
- VLAN type
- VLAN state
- Additional VLAN configuration information specific to the VLAN type

In VTP version 3, VTP advertisements also include the primary server ID, an instance number, and a start index.

Related Topics

Prerequisites for VTP, on page 1449

VTP Version 2

If you use VTP in your network, you must decide which version of VTP to use. By default, VTP operates in version 1.

VTP version 2 supports these features that are not supported in version 1:

- Token Ring support—VTP version 2 supports Token Ring Bridge Relay Function (TrBRF) and Token Ring Concentrator Relay Function (TrCRF) VLANs.
- Unrecognized Type-Length-Value (TLV) support—A VTP server or client propagates configuration changes to its other trunks, even for TLVs it is not able to parse. The unrecognized TLV is saved in NVRAM when the switch is operating in VTP server mode.
- Version-Dependent Transparent Mode—In VTP version 1, a VTP transparent switch inspects VTP messages for the domain name and version and forwards a message only if the version and domain name match. Although VTP version 2 supports only one domain, a VTP version 2 transparent switch forwards a message only when the domain name matches.
- Consistency Checks—In VTP version 2, VLAN consistency checks (such as VLAN names and values) are performed only when you enter new information through the CLI or SNMP. Consistency checks are not performed when new information is obtained from a VTP message or when information is read from NVRAM. If the MD5 digest on a received VTP message is correct, its information is accepted.

Related Topics

Enabling the VTP Version (CLI), on page 1462

VTP Version 3

VTP version 3 supports these features that are not supported in version 1 or version 2:

- Enhanced authentication—You can configure the authentication as **hidden** or **secret**. When **hidden**, the secret key from the password string is saved in the VLAN database file, but it does not appear in plain text in the configuration. Instead, the key associated with the password is saved in hexadecimal format in the running configuration. You must reenter the password if you enter a takeover command in the domain. When you enter the **secret** keyword, you can directly configure the password secret key.
- Support for extended range VLAN (VLANs 1006 to 4094) database propagation—VTP versions 1 and 2 propagate only VLANs 1 to 1005.

  Note VTP pruning still applies only to VLANs 1 to 1005, and VLANs 1002 to 1005 are still reserved and cannot be modified.

- Support for any database in a domain—In addition to propagating VTP information, version 3 can propagate Multiple Spanning Tree (MST) protocol database information. A separate instance of the VTP protocol runs for each application that uses VTP.
- VTP primary server and VTP secondary servers—A VTP primary server updates the database information and sends updates that are honored by all devices in the system. A VTP secondary server can only back up the updated VTP configurations received from the primary server to its NVRAM.

  By default, all devices come up as secondary servers. You can enter the **vtp primary** privileged EXEC command to specify a primary server. Primary server status is only needed for database updates when the administrator issues a takeover message in the domain. You can have a working VTP domain without any primary servers. Primary server status is lost if the device reloads or domain parameters change, even when a password is configured on the switch.
- The option to turn VTP on or off on a per-trunk (per-port) basis—You can enable or disable VTP per port by entering the [**no**] **vtp** interface configuration command. When you disable VTP on trunking ports, all VTP instances for that port are disabled. You cannot set VTP to *off* for the MST database and *on* for the VLAN database on the same port.

  When you globally set VTP mode to off, it applies to all the trunking ports in the system. However, you can specify on or off on a per-VTP instance basis. For example, you can configure the switch as a VTP server for the VLAN database but with VTP *off* for the MST database.

Related Topics

Enabling the VTP Version (CLI), on page 1462

VTP Pruning

VTP pruning increases network available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to reach the destination devices. Without VTP pruning, a switch floods broadcast, multicast, and unknown unicast traffic across all trunk links within a VTP domain even though receiving switches might discard them. VTP pruning is disabled by default.

VTP pruning blocks unneeded flooded traffic to VLANs on trunk ports that are included in the pruning-eligible list. Only VLANs included in the pruning-eligible list can be pruned. By default, VLANs 2 through 1001 are pruning eligible switch trunk ports. If the VLANs are configured as pruning-ineligible, the flooding continues. VTP pruning is supported in all VTP versions.

Figure 72: Flooding Traffic without VTP Pruning

VTP pruning is disabled in the switched network. Port 1 on Switch A and Port 2 on Switch D are assigned to the Red VLAN. If a broadcast is sent from the host connected to Switch A, Switch A floods the broadcast and every switch in the network receives it, even though Switches C, E, and F have no ports in the Red VLAN.

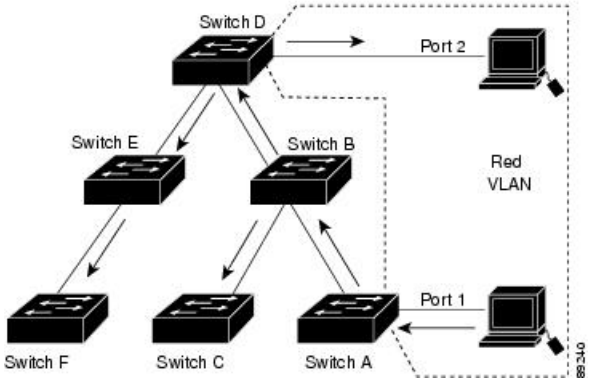
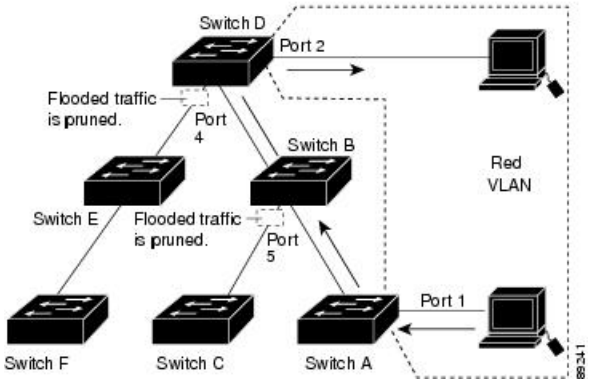


Figure 73: Optimized Flooded Traffic VTP Pruning

VTP pruning is enabled in the switched network. The broadcast traffic from Switch A is not forwarded to Switches C, E, and F because traffic for the Red VLAN has been pruned on the links shown (Port 5 on Switch B and Port 4 on Switch D).



With VTP versions 1 and 2, when you enable pruning on the VTP server, it is enabled for the entire VTP domain. In VTP version 3, you must manually enable pruning on each switch in the domain. Making VLANs pruning-eligible or pruning-ineligible affects pruning eligibility for those VLANs on that trunk only (not on all switches in the VTP domain).

VTP pruning takes effect several seconds after you enable it. VTP pruning does not prune traffic from VLANs that are pruning-ineligible. VLAN 1 and VLANs 1002 to 1005 are always pruning-ineligible; traffic from these VLANs cannot be pruned. Extended-range VLANs (VLAN IDs higher than 1005) are also pruning-ineligible.

Related Topics

Enabling VTP Pruning (CLI), on page 1464

VTP Configuration Guidelines

VTP Configuration Requirements

When you configure VTP, you must configure a trunk port so that the switch can send and receive VTP advertisements to and from other switches in the domain.

VTP Settings

The VTP information is saved in the VTP VLAN database. When VTP mode is transparent, the VTP domain name and mode are also saved in the switch running configuration file, and you can save it in the switch startup configuration file by entering the **copy running-config startup-config** privileged EXEC command. You must use this command if you want to save VTP mode as transparent, even if the switch resets.

When you save VTP information in the switch startup configuration file and reboot the switch, the switch configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for VLAN IDs 1 to 1005 use the VLAN database information.

Related Topics

Configuring VTP on a Per-Port Basis (CLI), on page 1465
Configuring a VTP Version 3 Primary Server (CLI), on page 1461

Domain Names for Configuring VTP

When configuring VTP for the first time, you must always assign a domain name. You must configure all switches in the VTP domain with the same domain name. Switches in VTP transparent mode do not exchange VTP messages with other switches, and you do not need to configure a VTP domain name for them.

Note If the NVRAM and DRAM storage is sufficient, all switches in a VTP domain should be in VTP server mode.

Caution Do not configure a VTP domain if all switches are operating in VTP client mode. If you configure the domain, it is impossible to make changes to the VLAN configuration of that domain. Make sure that you configure at least one switch in the VTP domain for VTP server mode.

Related Topics

Adding a VTP Client Switch to a VTP Domain (CLI), on page 1466

Passwords for the VTP Domain

You can configure a password for the VTP domain, but it is not required. If you do configure a domain password, all domain switches must share the same password and you must configure the password on each switch in the management domain. Switches without a password or with the wrong password reject VTP advertisements.

If you configure a VTP password for a domain, a switch that is booted without a VTP configuration does not accept VTP advertisements until you configure it with the correct password. After the configuration, the switch accepts the next VTP advertisement that uses the same password and domain name in the advertisement.

If you are adding a new switch to an existing network with VTP capability, the new switch learns the domain name only after the applicable password has been configured on it.

Caution When you configure a VTP domain password, the management domain does not function properly if you do not assign a management domain password to each switch in the domain.

Related Topics

Configuring a VTP Version 3 Password (CLI), on page 1460
Example: Configuring a Switch as the Primary Server, on page 1469

VTP Version

Follow these guidelines when deciding which VTP version to implement:

- All switches in a VTP domain must have the same domain name, but they do not need to run the same VTP version.
- A VTP version 2-capable switch can operate in the same VTP domain as a switch running VTP version 1 if version 2 is disabled on the version 2-capable switch (version 2 is disabled by default).
- If a switch running VTP version 1, but capable of running VTP version 2, receives VTP version 3 advertisements, it automatically moves to VTP version 2.
- If a switch running VTP version 3 is connected to a switch running VTP version 1, the VTP version 1 switch moves to VTP version 2, and the VTP version 3 switch sends scaled-down versions of the VTP packets so that the VTP version 2 switch can update its database.
- A switch running VTP version 3 cannot move to version 1 or 2 if it has extended VLANs.
- Do not enable VTP version 2 on a switch unless all of the switches in the same VTP domain are version-2-capable. When you enable version 2 on a switch, all of the version-2-capable switches in the domain enable version 2. If there is a version 1-only switch, it does not exchange VTP information with switches that have version 2 enabled.
- Cisco recommends placing VTP version 1 and 2 switches at the edge of the network because they do not forward VTP version 3 advertisements.
- If there are TrBRF and TrCRF Token Ring networks in your environment, you must enable VTP version 2 or version 3 for Token Ring VLAN switching to function properly. To run Token Ring and Token Ring-Net, disable VTP version 2.

- VTP version 1 and version 2 do not propagate configuration information for extended range VLANs (VLANs 1006 to 4094). You must configure these VLANs manually on each device. VTP version 3 supports extended-range VLANs and support for extended range VLAN database propagation.
- When a VTP version 3 device trunk port receives messages from a VTP version 2 device, it sends a scaled-down version of the VLAN database on that particular trunk in VTP version 2 format. A VTP version 3 device does not send VTP version 2-formatted packets on a trunk unless it first receives VTP version 2 packets on that trunk port.
- When a VTP version 3 device detects a VTP version 2 device on a trunk port, it continues to send VTP version 3 packets, in addition to VTP version 2 packets, to allow both kinds of neighbors to coexist on the same trunk.
- A VTP version 3 device does not accept configuration information from a VTP version 2 or version 1 device.
- Two VTP version 3 regions can only communicate in transparent mode over a VTP version 1 or version 2 region.
- Devices that are only VTP version 1 capable cannot interoperate with VTP version 3 devices.
- VTP version 1 and version 2 do not propagate configuration information for extended range VLANs (VLANs 1006 to 4094). You must manually configure these VLANs on each device.

Related Topics

Enabling the VTP Version (CLI), on page 1462

How to Configure VTP

Configuring VTP Mode (CLI)

You can configure VTP mode as one of these:

- VTP server mode—In VTP server mode, you can change the VLAN configuration and have it propagated throughout the network.
- VTP client mode—In VTP client mode, you cannot change its VLAN configuration. The client switch receives VTP updates from a VTP server in the VTP domain and then modifies its configuration accordingly.
- VTP transparent mode—In VTP transparent mode, VTP is disabled on the switch. The switch does not send VTP updates and does not act on VTP updates received from other switch. However, a VTP transparent switch running VTP version 2 does forward received VTP advertisements on its trunk links.
- VTP off mode—VTP off mode is the same as VTP transparent mode except that VTP advertisements are not forwarded.

When you configure a domain name, it cannot be removed; you can only reassign a switch to a different domain.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**vtp domain** *domain-name* **Example:** `Switch(config)# vtp domain eng_group`	Configures the VTP administrative-domain name. The name can be 1 to 32 characters. All switches operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name. This command is optional for modes other than server mode. VTP server mode requires a domain name. If the switch has a trunk connection to a VTP domain, the switch learns the domain name from the VTP server in the domain. You should configure the VTP domain before configuring other VTP parameters.
Step 4	**vtp mode** {**client** | **server** | **transparent** | **off**} {**vlan** | **mst** | **unknown**} **Example:** `Switch(config)# vtp mode server`	Configures the switch for VTP mode (client, server, transparent, or off). • **vlan**—The VLAN database is the default if none are configured. • **mst**—The multiple spanning tree (MST) database. • **unknown**—An unknown database type.
Step 5	**vtp password** *password* **Example:** `Switch(config)# vtp password mypassword`	(Optional) Sets the password for the VTP domain. The password can be 8 to 64 characters. If you configure a VTP password, the VTP domain does not function properly if you do not assign the same password to each switch in the domain.
Step 6	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Switch(config)# end`	
Step 7	**show vtp status** **Example:** `Switch# show vtp status`	Verifies your entries in the *VTP Operating Mode* and the *VTP Domain Name* fields of the display.
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves the configuration in the startup configuration file. Only VTP mode and domain name are saved in the switch running configuration and can be copied to the startup configuration file.

Related Topics

VTP Modes, on page 1451

Configuring a VTP Version 3 Password (CLI)

You can configure a VTP version 3 password on the switch.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**vtp version 3** **Example:** `Switch(config)# vtp version 3`	Enables VTP version 3 on the device. The default is VTP version 1.
Step 4	**vtp password** *password* [**hidden** | **secret**] **Example:**	(Optional) Sets the password for the VTP domain. The password can be 8 to 64 characters.

	Command or Action	Purpose
	`Switch(config)# vtp password mypassword hidden`	• (Optional) **hidden**—Saves the secret key generated from the password string in the nvram:vlan.dat file. If you configure a takeover by configuring a VTP primary server, you are prompted to reenter the password. • (Optional) **secret**—Directly configures the password. The secret password must contain 32 hexadecimal characters.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show vtp password** **Example:** `Switch# show vtp password`	Verifies your entries. The output appears like this: VTP password: 89914640C8D90868B6A0D8103847A733
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Passwords for the VTP Domain, on page 1457
Example: Configuring a Switch as the Primary Server, on page 1469

Configuring a VTP Version 3 Primary Server (CLI)

When you configure a VTP server as a VTP primary server, the takeover operation starts.

Procedure

	Command or Action	Purpose
Step 1	**vtp version 3** **Example:** `Switch(config)# vtp version 3`	Enables VTP version 3 on the device. The default is VTP version 1.

	Command or Action	Purpose
Step 2	**vtp primary** [**vlan** | **mst**] [**force**] **Example:** `Switch# vtp primary vlan force`	Changes the operational state of a switch from a secondary server (the default) to a primary server and advertises the configuration to the domain. If the switch password is configured as **hidden**, you are prompted to reenter the password. • (Optional) **vlan**—Selects the VLAN database as the takeover feature. This is the default. • (Optional) **mst**—Selects the multiple spanning tree (MST) database as the takeover feature. • (Optional) **force**—Overwrites the configuration of any conflicting servers. If you do not enter **force**, you are prompted for confirmation before the takeover.

Related Topics

VTP Settings, on page 1456

Enabling the VTP Version (CLI)

VTP version 2 and version 3 are disabled by default.

- When you enable VTP version 2 on a switch , every VTP version 2-capable switch in the VTP domain enables version 2. To enable VTP version 3, you must manually configure it on each switch .
- With VTP versions 1 and 2, you can configure the version only on switches in VTP server or transparent mode. If a switch is running VTP version 3, you can change to version 2 when the switch is in client mode if no extended VLANs exist, and no hidden password was configured.

Caution VTP version 1 and VTP version 2 are not interoperable on switches in the same VTP domain. Do not enable VTP version 2 unless every switch in the VTP domain supports version 2.

- In TrCRF and TrBRF Token Ring environments, you must enable VTP version 2 or VTP version 3 for Token Ring VLAN switching to function properly. For Token Ring and Token Ring-Net media, disable VTP version 2.
- 

Caution In VTP version 3, both the primary and secondary servers can exist on an instance in the domain.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**vtp version** {**1** | **2** | **3**} **Example:** `Switch(config)# vtp version 2`	Enables the VTP version on the switch. The default is VTP version 1.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show vtp status** **Example:** `Switch# show vtp status`	Verifies that the configured VTP version is enabled.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

VTP Version, on page 1457
VTP Version 2, on page 1453
VTP Version 3, on page 1453

Enabling VTP Pruning (CLI)

Before you begin

VTP pruning is not designed to function in VTP transparent mode. If one or more switches in the network are in VTP transparent mode, you should do one of these actions:

- Turn off VTP pruning in the entire network.
- Turn off VTP pruning by making all VLANs on the trunk of the switch upstream to the VTP transparent switch pruning ineligible.

To configure VTP pruning on an interface, use the **switchport trunk pruning vlan** interface configuration command. VTP pruning operates when an interface is trunking. You can set VLAN pruning-eligibility, whether or not VTP pruning is enabled for the VTP domain, whether or not any given VLAN exists, and whether or not the interface is currently trunking.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**vtp pruning** **Example:** `Switch(config)# vtp pruning`	Enables pruning in the VTP administrative domain. By default, pruning is disabled. You need to enable pruning on only one switch in VTP server mode.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show vtp status** **Example:** `Switch# show vtp status`	Verifies your entries in the *VTP Pruning Mode* field of the display.

Related Topics

VTP Pruning, on page 1454

Configuring VTP on a Per-Port Basis (CLI)

With VTP version 3, you can enable or disable VTP on a per-port basis. You can enable VTP only on ports that are in trunk mode. Incoming and outgoing VTP traffic are blocked, not forwarded.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/1`	Identifies an interface, and enters interface configuration mode.
Step 4	**vtp** **Example:** `Switch(config-if)# vtp`	Enables VTP on the specified port.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config interface** *interface-id* **Example:** `Switch# show running-config interface gigabitethernet1/0/1`	Verifies the change to the port.

	Command or Action	Purpose
Step 7	**show vtp status** **Example:** `Switch# show vtp status`	Verifies the configuration.

Related Topics

VTP Settings, on page 1456

Adding a VTP Client Switch to a VTP Domain (CLI)

Follow these steps to verify and reset the VTP configuration revision number on a switch *before* adding it to a VTP domain.

Before you begin

Before adding a VTP client to a VTP domain, always verify that its VTP configuration revision number is *lower* than the configuration revision number of the other switches in the VTP domain. Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number. With VTP versions 1 and 2, adding a switch that has a revision number higher than the revision number in the VTP domain can erase all VLAN information from the VTP server and VTP domain. With VTP version 3, the VLAN information is not erased.

You can use the **vtp mode transparent** global configuration command to disable VTP on the switch and then to change its VLAN information without affecting the other switches in the VTP domain.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show vtp status** **Example:** `Switch# show vtp status`	Checks the VTP configuration revision number. If the number is 0, add the switch to the VTP domain. If the number is greater than 0, follow these substeps: • Write down the domain name. • Write down the configuration revision number.

	Command or Action	Purpose
		• Continue with the next steps to reset the switch configuration revision number.
Step 3	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 4	**vtp domain** *domain-name* **Example:** `Switch(config)# vtp domain domain123`	Changes the domain name from the original one displayed in Step 1 to a new name.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. The VLAN information on the switch is updated and the configuration revision number is reset to 0.
Step 6	**show vtp status** **Example:** `Switch# show vtp status`	Verifies that the configuration revision number has been reset to 0.
Step 7	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 8	**vtp domain** *domain-name* **Example:** `Switch(config)# vtp domain domain012`	Enters the original domain name on the switch
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. The VLAN information on the switch is updated.

	Command or Action	Purpose
Step 10	**show vtp status** **Example:** `Switch# show vtp status`	(Optional) Verifies that the domain name is the same as in Step 1 and that the configuration revision number is 0.

Related Topics

VTP Domain, on page 1450
Prerequisites for VTP, on page 1449
Domain Names for Configuring VTP, on page 1456

Monitoring VTP

This section describes commands used to display and monitor the VTP configuration.

You monitor VTP by displaying VTP configuration information: the domain name, the current VTP revision, and the number of VLANs. You can also display statistics about the advertisements sent and received by the switch.

Table 118: VTP Monitoring Commands

Command	Purpose
show vtp counters	Displays counters about VTP messages that have been sent and received.
show vtp devices [**conflict**]	Displays information about all VTP version 3 devices in the domain. Conflicts are VTP version 3 devices with conflicting primary servers. The **show vtp devices** command does not display information when the switch is in transparent or off mode.
show vtp interface [*interface-id*]	Displays VTP status and configuration for all interfaces or the specified interface.
show vtp password	Displays the VTP password. The form of the password displayed depends on whether or not the **hidden** keyword was entered and if encryption is enabled on the switch.
show vtp status	Displays the VTP switch configuration information.

Configuration Examples for VTP

Example: Configuring a Switch as the Primary Server

This example shows how to configure a switch as the primary server for the VLAN database (the default) when a hidden or secret password was configured:

```
Switch# vtp primary vlan
Enter VTP password: mypassword
This switch is becoming Primary server for vlan feature in the VTP  domain

VTP Database Conf Switch ID      Primary Server Revision System Name
------------ ---- -------------- -------------- -------- --------------------
VLANDB       Yes  00d0.00b8.1400=00d0.00b8.1400 1        stp7

Do you want to continue (y/n) [n]? y
```

Related Topics

Configuring a VTP Version 3 Password (CLI), on page 1460
Passwords for the VTP Domain, on page 1457

Where to Go Next

After configuring VTP, you can configure the following:

- VLANs
- VLAN groups
- VLAN trunking

Additional References

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	*VLAN Command Reference (Catalyst 3850 Switches) VLAN Command Reference (Cisco WLC 5700 Series)* *Layer 2/3 Command Reference (Catalyst 3850 Switches)Layer 2 Command Reference (Cisco WLC 5700 Series)*
Additional configuration commands and procedures.	*LAN Switching Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)* *Layer 2/3 Configuration Guide (Catalyst 3850 Switches)Layer 2 Configuration Guide (Cisco WLC 5700 Series)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIBs

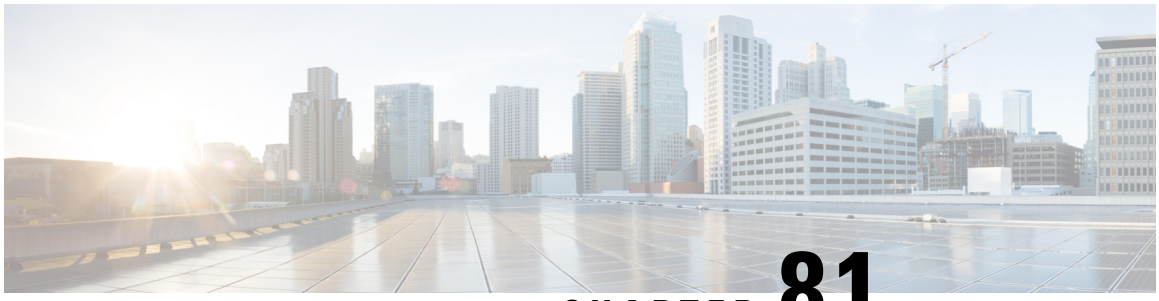
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for VTP

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 81

Configuring VLANs

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VLANs

The following are prerequisites and considerations for configuring VLANs:

- Before you create VLANs, you must decide whether to use VLAN Trunking Protocol (VTP) to maintain global VLAN configuration for your network.
- If you plan to configure many VLANs on the switch and to not enable routing, you can set the Switch Database Management (SDM) feature to the VLAN template, which configures system resources to support the maximum number of unicast MAC addresses.
- Switches running the LAN Base feature set support only static routing on SVIs.
- A VLAN should be present in the switch to be able to add it to the VLAN group.

Restrictions for VLANs

The following are restrictions for VLANs:

- The switch supports per-VLAN spanning-tree plus (PVST+) or rapid PVST+ with a maximum of 128 spanning-tree instances in the Cisco Catalyst 9500 Series Switches. One spanning-tree instance is allowed per VLAN.
- The switch supports IEEE 802.1Q trunking methods for sending VLAN traffic over Ethernet ports.
- Configuring an interface VLAN router's MAC address is not supported. The interface VLAN already has an MAC address assigned by default.
- Private VLANs are not supported on the switch.
- You cannot have a switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches.

Information About VLANs

Logical Networks

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or a switch supporting fallback bridging. Because a VLAN is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information and can support its own implementation of spanning tree.

VLANs are often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the switch is assigned manually on an interface-by-interface basis. When you assign switch interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

Traffic between VLANs must be routed.

The switch can route traffic between VLANs by using switch virtual interfaces (SVIs). An SVI must be explicitly configured and assigned an IP address to route traffic between VLANs.

Supported VLANs

The switch supports VLANs in VTP client, server, and transparent modes. VLANs are identified by a number from 1 to 4094. VLAN 1 is the default VLAN and is created during system initialization. VLAN IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs. All of the VLANs except 1002 to 1005 are available for user configuration.

There are 3 VTP versions: VTP version 1, version 2, and version 3. All VTP versions support both normal and extended range VLANs, but only with VTP version 3, does the switch propagate extended range VLAN configuration information. When extended range VLANs are created in VTP versions 1 and 2, their

configuration information is not propagated. Even the local VTP database entries on the switch are not updated, but the extended range VLANs configuration information is created and stored in the running configuration file.

You can configure up to 4094 VLANs on the switch.

VLAN Port Membership Modes

You configure a port to belong to a VLAN by assigning a membership mode that specifies the kind of traffic the port carries and the number of VLANs to which it can belong.

When a port belongs to a VLAN, the switch learns and manages the addresses associated with the port on a per-VLAN basis.

Table 119: Port Membership Modes and Characteristics

Membership Mode	VLAN Membership Characteristics	VTP Characteristics
Static-access	A static-access port can belong to one VLAN and is manually assigned to that VLAN.	VTP is not required. If you do not want VTP to globally propagate information, set the VTP mode to transparent. To participate in VTP, there must be at least one trunk port on the switch connected to a trunk port of a second switch.
Trunk (IEEE 802.1Q) : • IEEE 802.1Q—Industry-standard trunking encapsulation.	A trunk port is a member of all VLANs by default, including extended-range VLANs, but membership can be limited by configuring the allowed-VLAN list. You can also modify the pruning-eligible list to block flooded traffic to VLANs on trunk ports that are included in the list.	VTP is recommended but not required. VTP maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP exchanges VLAN configuration messages with other switches over trunk links.
Voice VLAN	A voice VLAN port is an access port attached to a Cisco IP Phone, configured to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone.	VTP is not required; it has no effect on a voice VLAN.

Related Topics

Assigning Static-Access Ports to a VLAN (CLI), on page 1480
Monitoring VLANs, on page 1487

VLAN Configuration Files

Configurations for VLAN IDs 1 to 1005 are written to the vlan.dat file (VLAN database), and you can display them by entering the **show vlan** privileged EXEC command. The vlan.dat file is stored in flash memory. If the VTP mode is transparent, they are also saved in the switch running configuration file.

You use the interface configuration mode to define the port membership mode and to add and remove ports from VLANs. The results of these commands are written to the running-configuration file, and you can display the file by entering the **show running-config** privileged EXEC command.

When you save VLAN and VTP information (including extended-range VLAN configuration information) in the startup configuration file and reboot the switch, the switch configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration, and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration does not match the VLAN database, the domain name and VTP mode and configuration for the VLAN IDs 1 to 1005 use the VLAN database information.
- In VTP versions 1 and 2, if VTP mode is server, the domain name and VLAN configuration for VLAN IDs 1 to 1005 use the VLAN database information. VTP version 3 also supports VLANs 1006 to 4094.
- From image 15.0(02)SE6, on vtp transparent and off modes, vlans get created from startup-config even if they are not applied to the interface.

Note Ensure that you delete the vlan.dat file along with the configuration files before you reset the switch configuration using **write erase** command. This ensures that the switch reboots correctly on a reset.

Normal-Range VLAN Configuration Guidelines

Normal-range VLANs are VLANs with IDs from 1 to 1005.

Follow these guidelines when creating and modifying normal-range VLANs in your network:

- Normal-range VLANs are identified with a number between 1 and 1001. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs.
- VLAN configurations for VLANs 1 to 1005 are always saved in the VLAN database. If the VTP mode is transparent, VTP and VLAN configurations are also saved in the switch running configuration file.
- If the switch is in VTP server or VTP transparent mode, you can add, modify or remove configurations for VLANs 2 to 1001 in the VLAN database. (VLAN IDs 1 and 1002 to 1005 are automatically created and cannot be removed.)
- Extended-range VLANs created in VTP transparent mode are not saved in the VLAN database and are not propagated. VTP version 3 supports extended range VLAN (VLANs 1006 to 4094) database propagation in VTP server mode.
- Before you can create a VLAN, the switch must be in VTP server mode or VTP transparent mode. If the switch is a VTP server, you must define a VTP domain or VTP will not function.
- The switch does not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic, but it does propagate the VLAN configuration through VTP.

- The switch supports 128 spanning tree instances. If a switch has more active VLANs than supported spanning-tree instances, spanning tree can be enabled on 128 VLANs and is disabled on the remaining VLANs.

  If you have already used all available spanning-tree instances on a switch, adding another VLAN anywhere in the VTP domain creates a VLAN on that switch that is not running spanning-tree. If you have the default allowed list on the trunk ports of that switch (which is to allow all VLANs), the new VLAN is carried on all trunk ports. Depending on the topology of the network, this could create a loop in the new VLAN that would not be broken, particularly if there are several adjacent switches that all have run out of spanning-tree instances. You can prevent this possibility by setting allowed lists on the trunk ports of switches that have used up their allocation of spanning-tree instances.

  If the number of VLANs on the switch exceeds the number of supported spanning-tree instances, we recommend that you configure the IEEE 802.1s Multiple STP (MSTP) on your switch to map multiple VLANs to a single spanning-tree instance.

Related Topics

Creating or Modifying an Ethernet VLAN (CLI), on page 1476
Monitoring VLANs, on page 1487

Extended-Range VLAN Configuration Guidelines

Extended-range VLANs are VLANs with IDs from 1006 to 4094.

Follow these guidelines when creating extended-range VLANs:

- VLAN IDs in the extended range are not saved in the VLAN database and are not recognized by VTP unless the switch is running VTP version 3.
- You cannot include extended-range VLANs in the pruning eligible range.
- For VTP version 1 or 2, you can set the VTP mode to transparent in global configuration mode. You should save this configuration to the startup configuration so that the switch boots up in VTP transparent mode. Otherwise, you lose the extended-range VLAN configuration if the switch resets. If you create extended-range VLANs in VTP version 3, you cannot convert to VTP version 1 or 2.

Related Topics

Creating an Extended-Range VLAN (CLI), on page 1482
Monitoring VLANs, on page 1487

How to Configure VLANs

How to Configure Normal-Range VLANs

You can set these parameters when you create a new normal-range VLAN or modify an existing VLAN in the VLAN database:

- VLAN ID
- VLAN name

- VLAN type
  - Ethernet
  - Fiber Distributed Data Interface [FDDI]
  - FDDI network entity title [NET]
  - TrBRF or TrCRF
  - Token Ring
  - Token Ring-Net
- VLAN state (active or suspended)
- Security Association Identifier (SAID)
- Bridge identification number for TrBRF VLANs
- Ring number for FDDI and TrCRF VLANs
- Parent VLAN number for TrCRF VLANs
- Spanning Tree Protocol (STP) type for TrCRF VLANs
- VLAN number to use when translating from one VLAN type to another

You can cause inconsistency in the VLAN database if you attempt to manually delete the vlan.dat file. If you want to modify the VLAN configuration, follow the procedures in this section.

Creating or Modifying an Ethernet VLAN (CLI)

Before you begin

With VTP version 1 and 2, if the switch is in VTP transparent mode, you can assign VLAN IDs greater than 1006, but they are not added to the VLAN database.

The switch supports only Ethernet interfaces. Because FDDI and Token Ring VLANs are not locally supported, you only configure FDDI and Token Ring media-specific characteristics for VTP global advertisements to other switches.

Although the switch does not support Token Ring connections, a remote device with Token Ring connections could be managed from one of the supported switches. Switches running VTP Version 2 advertise information about these Token Ring VLANs:

- Token Ring TrBRF VLANs
- Token Ring TrCRF VLANs

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters the global configuration mode.

	Command or Action	Purpose
	`Switch# configure terminal`	
Step 2	**vlan** *vlan-id* **Example:** `Switch(config)# vlan 20`	Enters a VLAN ID, and enters VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. **Note** The available VLAN ID range for this command is 1 to 4094. Additional **vlan** command options include: • **access-map**—Creates VLAN access-maps or enters the vlan access map command mode. • **configuration**—Enters the vlan feature configuration mode. • **dot1q**—Configures VLAN dot1q tag native parameters. • **filter**—Applies a VLAN filter map to a VLAN list. • **group**—Creates a VLAN group.
Step 3	**name** *vlan-name* **Example:** `Switch(config-vlan)# name test20`	(Optional) Enters a name for the VLAN. If no name is entered for the VLAN, the default is to append the *vlan-id* value with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4. The following additional VLAN configuration command options are available: • **are**—Sets the maximum number of All Router Explorer (ARE) hops for the VLAN. • **backupcrf**—Enables or disables the backup concentrator relay function (CRF) mode for the VLAN. • **bridge**—Sets the value of the bridge number for the FDDI net or Token Ring net type VLANs. • **exit**—Applies changes, bumps the revision number, and exits. • **media**—Sets the media type of the VLAN.

	Command or Action	Purpose
		• **no**—Negates the command or default. • **parent**—Sets the value of the ID for the parent VLAN for FDDI or Token Ring type VLANs. • **remote-span**—Configures a remote SPAN VLAN. • **ring**—Sets the ring number value for FDDI or Token Ring type VLANs. • **said**—Sets the IEEE 802.10 SAID value. • **shutdown**—Shuts down the VLAN switching. • **state**—Sets the operational VLAN state to active or suspended. • **ste**—Sets the maximum number of Spanning Tree Explorer (STE) hops for the VLAN. • **stp**—Sets the Spanning Tree characteristics of the VLAN.
Step 4	**media** { **ethernet** | **fd-net** | **fddi** | **tokenring** | **trn-net** } **Example:** `Switch(config-vlan)# media ethernet`	Configures the VLAN media type. Command options include: • **ethernet**—Sets the VLAN media type as Ethernet. • **fd-net**—Sets the VLAN media type as FDDI net. • **fddi**—Sets the VLAN media type as FDDI. • **tokenring**—Sets the VLAN media type as Token Ring. • **trn-net**—Sets the VLAN media type as Token Ring net.
Step 5	**remote-span** **Example:** `Switch(config-vlan)# remote-span`	(Optional) Configures the VLAN as the RSPAN VLAN for a remote SPAN session. For more information on remote SPAN, see the *Catalyst 3850 Network Management Configuration Guide*.
Step 6	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Switch(config)# end`	
Step 7	**show vlan** {**name** *vlan-name* | **id** *vlan-id*} **Example:** `Switch# show vlan name test20 id 20`	Verifies your entries.

Related Topics

Normal-Range VLAN Configuration Guidelines, on page 1474
Monitoring VLANs, on page 1487

Deleting a VLAN (CLI)

When you delete a VLAN from a switch that is in VTP server mode, the VLAN is removed from the VLAN database for all switches in the VTP domain. When you delete a VLAN from a switch that is in VTP transparent mode, the VLAN is deleted only on that specific switch .

You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.

Caution When you delete a VLAN, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**no vlan** *vlan-id* **Example:** `Switch(config)# no vlan 4`	Removes the VLAN by entering the VLAN ID.

	Command or Action	Purpose
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show vlan brief** **Example:** `Switch# show vlan brief`	Verifies the VLAN removal.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Monitoring VLANs, on page 1487

Assigning Static-Access Ports to a VLAN (CLI)

You can assign a static-access port to a VLAN without having VTP globally propagate VLAN configuration information by disabling VTP (VTP transparent mode).

For the Cisco Catalyst 9500 Series Switches, if you are assigning a port on a cluster member switch to a VLAN, first use the **rcommand** privileged EXEC command to log in to the cluster member switch.

If you assign an interface to a VLAN that does not exist, the new VLAN is created.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode
Step 3	**interface** *interface-id* **Example:**	Enters the interface to be added to the VLAN.

	Command or Action	Purpose
	`Switch(config)# interface gigabitethernet2/0/1`	
Step 4	**switchport mode access** **Example:** `Switch(config-if)# switchport mode access`	Defines the VLAN membership mode for the port (Layer 2 access port).
Step 5	**switchport access vlan** *vlan-id* **Example:** `Switch(config-if)# switchport access vlan 2`	Assigns the port to a VLAN. Valid VLAN IDs are 1 to 4094.
Step 6	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config interface** *interface-id* **Example:** `Switch# show running-config interface gigabitethernet2/0/1`	Verifies the VLAN membership mode of the interface.
Step 8	**show interfaces** *interface-id* **switchport** **Example:** `Switch# show interfaces gigabitethernet2/0/1 switchport`	Verifies your entries in the *Administrative Mode* and the *Access Mode VLAN* fields of the display.
Step 9	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

VLAN Port Membership Modes, on page 1473
Monitoring VLANs, on page 1487

How to Configure Extended-Range VLANs

Extended-range VLANs enable service providers to extend their infrastructure to a greater number of customers. The extended-range VLAN IDs are allowed for any **switchport** commands that allow VLAN IDs.

With VTP version 1 or 2, extended-range VLAN configurations are not stored in the VLAN database, but because VTP mode is transparent, they are stored in the switch running configuration file, and you can save the configuration in the startup configuration file. Extended-range VLANs created in VTP version 3 are stored in the VLAN database.

You can change only the MTU size and the remote SPAN configuration state on extended-range VLANs; all other characteristics must remain at the default state.

Creating an Extended-Range VLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

Step 3	**vlan** *vlan-id*
	Example:
	`Switch(config)# vlan 2000`
	`Switch(config-vlan)#`
		Enters an extended-range VLAN ID and enters VLAN configuration mode. The range is 1006 to 4094.

Step 4	**remote-span** **Example:** `Switch(config-vlan)# remote-span`	(Optional) Configures the VLAN as the RSPAN VLAN.

Step 5	**exit**
	Example:
	`Switch(config-vlan)# exit`
	`Switch(config)#`
		Returns to configuration mode.

	Command or Action	Purpose

Step 6	**interface vlan**
	Example:
	`Switch(config)# interface vlan 200`
	`Switch(config-if)#`
		Enters the interface configuration mode for the selected VLAN.

Step 7	**ip mtu** *mtu-size*
	Example:
	`Switch(config-if)# ip mtu 1024`
	`Switch(config-if)#`
		(Optional) Modifies the VLAN by changing the MTU size. You can configure the MTU size between 68 to 1500 bytes.
		Note Although all VLAN commands appear in the CLI help, only the **ip mtu** *mtu-size* and **remote-span** commands are supported for extended-range VLANs.

Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 9	**show vlan id** *vlan-id* **Example:** `Switch# show vlan id 2000`	Verifies that the VLAN has been created.
Step 10	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Extended-Range VLAN Configuration Guidelines, on page 1475
Monitoring VLANs, on page 1487

How to Configure VLANs (GUI)

Creating Layer2 VLAN (GUI)

To create a Layer2 VLAN using the switch web UI, you must follow the steps defined in this procedure.

Procedure

Step 1 To create a Layer2 VLAN, choose **Configuration > Controller > System > VLAN** > **Layer2 VLAN.**

The VLAN Layer2 page appears. You must provide values for all parameters listed in the Layer2 page.

Parameter	Description
VLAN ID	VLAN tag identifier, or 0 for no VLAN tag.
Name	VLAN name.
State	VLAN state. Values are the following: • Active • Suspended

Step 2 Click **Apply.**

Creating Layer3 Interface (GUI)

To create a Layer3 interface using the switch web UI, you must follow the steps defined in this procedure.

Procedure

Step 1 To create a Layer3 interface, choose **Configuration > Controller > System > VLAN** > **Layer3 Interface.**

The Layer3 interface page appears. You must provide values for all parameters listed in the window.

Parameter	Description
Description	Description for the Layer3 interface.
DHCP Relay Information	Information on controller built-in DHCP relay agents.
IP Address	IP address/subnet mask of the VLAN SVI (Switch Virtual Interface).
Mask Address	Mask address of the DHCP server.
IPv6 Address	IPv6 address of the DHCP server.
IPv4 DHCP Server	IPv4 address of the DHCP server.
IPv6 DHCP Server	IPv6 address of the DHCP server.

Step 2 Click **Apply.**

Viewing Layer2 VLAN (GUI)

You can view the details of the Layer2 VLANs configured in the switch interface using the web UI.

Procedure

	Command or Action	Purpose
Step 1	Choose **Configuration > Controller > System > VLAN** > **Layer2 VLAN .**	The Layer2 VLAN page appears, listing the following details of the Layer2 VLANs in the switch.

Parameter	Description
VLAN ID	Displays VLAN tag identifier.
Name	VLAN name.
State	VLAN state. Values are as follows: • Active • Suspended
MTU	Maximum transmission unit.

Viewing Layer3 Interface (GUI)

You can view the details of the Layer3 interfaces configured in the switch interface using the web UI.

Procedure

Choose **Configuration > Controller > System > VLAN** > **Layer3 Interface .**

The Layer2 VLAN page appears, listing the following details of the Layer3 interfaces in the switch.

Parameter	Description
Interface Name	Layer3 interface name.
Status	Status of the Layer3 interface. Values are the following: • Up • Down
Protocol	Protocol used for Layer3 interface.
IP Address	IP address used for Layer3 security and mobility managers.

Removing Layer2 VLAN (GUI)

To remove a Layer2 VLANs using the switch web UI, you must:

Procedure

Step 1 Choose **Configuration > Controller > System > VLAN** > **Layer2 VLAN .**

The Layer2 VLAN page appears, listing the following details of the Layer2 VLANs associated with the switch.

Parameter	Description
VLAN ID	Displays VLAN tag identifier.
Name	VLAN name.
State	VLAN state. Values are as follows: • Active • Suspended
MTU	Maximum transmission unit.

Step 2 Check the checkbox of the Layer2 VLAN you need to delete from the Layer2 VLANs displayed in the Layer2 VLAN list .

You will receive a confirmation message confirming deletion of the selected Layer2 VLAN.

Step 3 Click **Ok**.

Removing Layer3 Interface (GUI)

To remove a Layer3 interface using the switch web UI, you must:

Procedure

Step 1 Choose **Configuration > Controller > System > VLAN** > **Layer3 Interface.**

The Layer3 interface page appears, listing the following details of the Layer3 interfaces associated with the switch.

Parameter	Description
Interface Name	Layer3 interface name.
Status	Status of the Layer3 interface. Values are the following: • Up • Down
Protocol	Protocol used for Layer3 interface.
IP Address	IP address used for Layer3 security and mobility managers.

Step 2 Check the checkbox of the Layer3 interfaces you need to delete from the Layer3 interfaces displayed in the Layer3 interfaces.

You will receive a confirmation message confirming deletion of the selected Layer3 interface.

Step 3 Click **Ok**.

Monitoring VLANs

Table 120: Privileged EXEC show Commands

Command	Purpose
show interfaces [**vlan** *vlan-id*]	Displays characteristics for all interfaces or for the specified VLAN configured on the switch .
show vlan [**access-map** *name* | **brief** | **dot1q** { **tag native** } | **filter** [**access-map** | **vlan**] | **group** [**group-name** *name*] | **id** *vlan-id* | **ifindex** | **mtu** | **name** *name* | **remote-span** | **summary**]	Displays parameters for all VLANs or the specified VLAN on the switch. The following command options are available: • **access-map**—Displays the VLAN access-maps. • **brief**—Displays VTP VLAN status in brief. • **dot1q**—Displays the dot1q parameters. • **filter**—Displays VLAN filter information. • **group**—Displays the VLAN group with its name and the connected VLANs that are available. • **id**—Displays VTP VLAN status by identification number. • **ifindex**—Displays SNMP ifIndex. • **mtu**—Displays VLAN MTU information. • **name**—Displays the VTP VLAN information by specified name. • **remote-span**–Displays the remote SPAN VLANs. • **summary**—Displays a summary of VLAN information.

Related Topics

Creating or Modifying an Ethernet VLAN (CLI), on page 1476
Normal-Range VLAN Configuration Guidelines, on page 1474
Deleting a VLAN (CLI), on page 1479
Assigning Static-Access Ports to a VLAN (CLI), on page 1480
VLAN Port Membership Modes, on page 1473
Creating an Extended-Range VLAN (CLI), on page 1482
Extended-Range VLAN Configuration Guidelines, on page 1475

Where to Go Next

After configuring VLANs, you can configure the following:

- VLAN groups
- VLAN Trunking Protocol (VTP)
- VLAN trunks

Additional References

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	*VLAN Command Reference (Catalyst 3850 Switches) VLAN Command Reference (Cisco WLC 5700 Series)* *Layer 2/3 Command Reference (Catalyst 3850 Switches)Layer 2 Command Reference (Cisco WLC 5700 Series)*
VLAN access-maps	*Security Configuration Guide (Catalyst 3850 Switches)Security Configuration Guide (Cisco WLC 5700 Series)* *Security Command Reference (Catalyst 3850 Switches)Security Command Reference (Cisco WLC 5700 Series)*
VLAN and Mobility Agents	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
Cisco Flexible NetFlow	*Cisco Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)* *Flexible Netflow Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
IGMP Snooping	*IP Multicast Routing Command Reference (Catalyst 3850 Switches)Cisco 5760 Multicast Command Reference (Cisco WLC 5700 Series)* *IP Multicast Routing Configuration Guide (Catalyst 3850 Switches)Routing Configuration Guide (Cisco WLC 5700 Series)*
IPv6	*IPv6 Configuration Guide (Catalyst 3850 Switches)IPv6 Configuration Guide (Cisco WLC 5700 Series)* *IPv6 Command Reference (Catalyst 3850 Switches)IPv6 Command Reference (Cisco WLC 5700 Series)*

Related Topic	Document Title
SPAN	*Network Management Command Reference (Catalyst 3850 Switches)Network Management Command Reference (Cisco WLC 5700 Series)* *Network Management Configuration Guide (Catalyst 3850 Switches) Network Management Configuration Guide (Cisco WLC 5700 Series)*
Platform-independent configuration information	*Identity Based Networking Services Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIBs

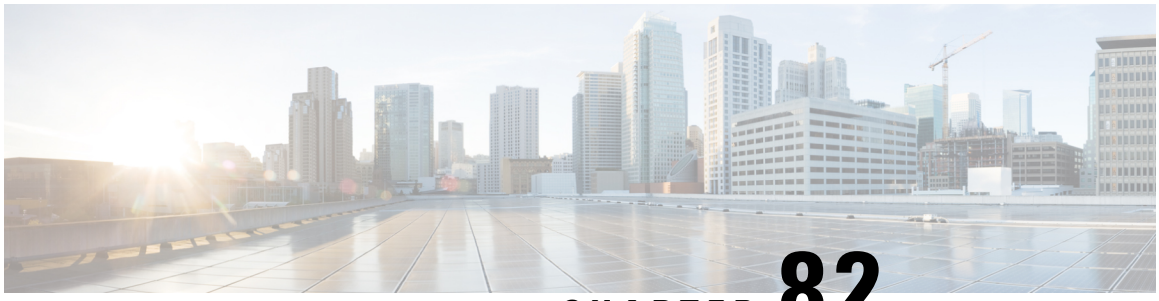
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for VLANs

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced
Cisco IOS XE 3.3SE	VLAN GUI support.
Cisco IOS XE Everest 16.5.1a	This feature was introduced.



CHAPTER 82

Configuring VLAN Groups

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VLAN Groups

- A VLAN should be present in the switch to be able to add it to the VLAN group.
- For VLAN group to function properly, in addition to enabling DHCP snooping globally, you must ensure that DHCP snooping is enabled in all the VLANs.

Restrictions for VLAN Groups

- The number of VLANs mapped to a VLAN group is not limited by Cisco IOS Software Release. But if the number of VLANs in a VLAN group exceed the recommended value of 32, the mobility behavior is unexpected and in the VLAN group, L2 multicast breaks for some VLANs. So it is the responsibility of the administrator to configure feasible number of VLANs in a VLAN group. When a VLAN is added to

a VLAN group mapped to a WLAN which already has 32 VLANs, a warning is generated. But when a new VLAN group is mapped to a WLAN with more than 32 VLANs, an error is generated.

For expected behavior of the VLAN group, the VLANs mapped in the group must be present in the switch. The static IP client behavior is not supported.

Information About VLAN Groups

Whenever a client connects to a wireless network (WLAN), the client is placed in a VLAN that is associated with the WLAN. In a large venue such as an auditorium, a stadium, or a conference room where there are numerous wireless clients, having only a single WLAN to accommodate many clients might be a challenge.

The VLAN group feature uses a single WLAN that can support multiple VLANs. The clients can get assigned to one of the configured VLANs. This feature maps a WLAN to a single VLAN or multiple VLANs using the VLAN groups. When a wireless client associates to the WLAN, the VLAN is derived by an algorithm based on the MAC address of the wireless client. A VLAN is assigned to the client and the client gets the IP address from the assigned VLAN. This feature also extends the current AP group architecture and AAA override architecture, where the AP groups and AAA override can override a VLAN or a VLAN group to which the WLAN is mapped.

When a client associates with a WLAN and the WLAN is applied to a VLAN group, an index is calculated based on the MAC address of the client and the number of VLANs in the VLAN group using a hash algorithm. Based on this index, a VLAN is assigned to the client. If the index is "dirty," another index is generated in a round-robin manner and the VLAN is assigned to the client based on the newly generated index.

The system marks VLAN as "dirty" for 30 minutes when the clients are unable to receive IP address using DHCP. The system might not clear the "dirty" flag from the VLAN even after 30 minutes for a VLAN group. After 30 minutes, when VLAN is marked non-dirty, new clients in IP Learn state can get assigned with IP address from the VLAN if free IPs are available in the pool and DHCP scope is defined correctly. This is expected behavior because the timestamp of each interface has to be checked to see if it is greater than 30 minutes, due to which there is a lag of 5 minutes for the global timer to expire.

Related Topics

Creating VLAN Groups (CLI), on page 1492

How to Configure VLAN Groups

Creating VLAN Groups (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.

	Command or Action	Purpose
Step 2	**vlan group** *WORD* **vlan-list** *vlan-ID* **Example:** `Switch(config)#vlan group vlangrp1 vlan-list 91-95`	Creates a VLAN group with the given group name (vlangrp1) and adds all the VLANs listed in the command. The VLAN list ranges from 1 to 4096 and the recommended number of VLANs in a group is 32.
Step 3	**end** **Example:** `Switch(config)#end`	Exits the global configuration mode and returns to privileged EXEC mode. Alternatively, press **CTRL-Z** to exit the global configuration mode.

Related Topics

Information About VLAN Groups, on page 1492

Removing VLAN Group (CLI)

Procedure

Step 1 **configure terminal**

Example:

```
Switch# configure terminal
```

Enters global command mode.

Step 2 **vlan group** *WORD* **vlan-list** *vlan-ID*

Example:

```
Switch(config)#vlan group vlangrp1 vlan-list 91-95
```

Creates a VLAN group with the given group name (vlangrp1) and adds all the VLANs listed in the command. The VLAN list ranges from 1 to 4096 and the recommended number of VLANs in a group is 32.

Step 3 **no vlan group** *WORD* **vlan-list** *vlan-ID*

Example:

```
Switch(config)#no vlan group vlangrp1 vlan-list 91-95
```

Removes the VLAN group with the given group name (vlangrp1).

Step 4 **end**

Example:

```
Switch(config)#end
```

Exits the global configuration mode and returns to privileged EXEC mode. Alternatively, press **CTRL-Z** to exit the global configuration mode.

Creating VLAN Groups (GUI)

To create a VLAN group using the switch web UI, you must:

Procedure

Step 1 Choose **Configuration > Controller > System > VLAN** > **VLAN Group.**

The VLAN Group page appears. You must provide values for all parameters listed in the VLAN Group window.

Parameter	Description
VLAN Group Name	Group name for the VLANs.
VLAN List	The VLAN list to configure the mesh access point (MAP) access port.

Step 2 Click **Apply**.

Adding a VLAN Group to WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 2	**wlan** *WORD number* **Example:** `Switch(config)#wlan wlanname 512`	Enables the WLAN to map a VLAN group using an identifier. The WLAN identifier values range from 1 to 512.
Step 3	**client vlan** *WORD* **Example:** `Switch(config-wlan)#client vlan vlangrp1`	Maps the VLAN group to the WLAN by entering the VLAN identifier, VLAN group, or the VLAN name.
Step 4	**end** **Example:** `Switch(config-wlan)#end`	Exits the global configuration mode and returns to privileged EXEC mode. Alternatively, press **CTRL-Z** to exit the global configuration mode.

Adding a VLAN Group to WLAN (GUI)

To add a VLAN group to WLAN using the switch web UI, you must follow the steps defined in this procedure.

Procedure

Step 1 To add a VLAN group to a WLAN, choose **Configuration > Wireless > WLANs > WLAN Profile > General.**

The general parameter page of the WLAN group appears.

Step 2 Select the VLAN group values listed in the **Interface/Interface Group** drop-down list to associate the selected WLAN profile to a VLAN group.

Step 3 Click **Apply.**

Removing VLAN Groups (GUI)

To remove a VLAN groups using the switch web UI, you must:

Procedure

Step 1 Choose **Configuration > Controller > System > VLAN** > **VLAN Group.**

The VLAN Group page appears, listing the following details of the VLAN groups associated with the switch.

Parameter	Description
VLAN Group Name	Group name for the VLANs.
VLAN List	The VLAN list to configure the mesh access point (MAP) access port.

Step 2 Check the checkbox of the VLAN group you need to delete from the VLAN group names displayed in the VLAN group list .

You will receive a confirmation message confirming deletion of the selected VLAN group.

Step 3 Click **Ok**.

Viewing VLANs in VLAN Groups (CLI)

Commands	Description
show vlan group	Displays the list of VLAN groups with its name and the VLANs that are available.
show vlan group group-name *group_name*	Displays the specified VLAN group details.
show wireless vlan group *group_name*	Displays the specified wireless VLAN group details.

Viewing VLAN Groups (GUI)

To view a VLAN groups using the switch web UI, you must:

Procedure

Step 1 Choose **Configuration > Controller > System > VLAN** > **VLAN Group.**

The VLAN Group page appears, listing the following details of the VLAN groups associated with the switch.

Parameter	Description
VLAN Group Name	Group name for the VLANs.
VLAN List	The VLAN list to configure the mesh access point (MAP) access port.

Step 2 Click **Apply**.

Where to Go Next

After configuring VLAN groups, you can configure the following:

- VLANs
- VLAN Trunking Protocol (VTP)
- VLAN trunks

Additional References

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	*VLAN Command Reference (Catalyst 3850 Switches) VLAN Command Reference (Cisco WLC 5700 Series)* *Layer 2/3 Command Reference (Catalyst 3850 Switches)Layer 2 Command Reference (Cisco WLC 5700 Series)*
VLAN access-maps	*Security Configuration Guide (Catalyst 3850 Switches)Security Configuration Guide (Cisco WLC 5700 Series)* *Security Command Reference (Catalyst 3850 Switches)Security Command Reference (Cisco WLC 5700 Series)*
VLAN and Mobility Agents	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
Cisco Flexible NetFlow	*Cisco Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)* *Flexible Netflow Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Related Topic	Document Title
IGMP Snooping	*IP Multicast Routing Command Reference (Catalyst 3850 Switches)Cisco 5760 Multicast Command Reference (Cisco WLC 5700 Series)* *IP Multicast Routing Configuration Guide (Catalyst 3850 Switches)Routing Configuration Guide (Cisco WLC 5700 Series)*
IPv6	*IPv6 Configuration Guide (Catalyst 3850 Switches)IPv6 Configuration Guide (Cisco WLC 5700 Series)* *IPv6 Command Reference (Catalyst 3850 Switches)IPv6 Command Reference (Cisco WLC 5700 Series)*
SPAN	*Network Management Command Reference (Catalyst 3850 Switches)Network Management Command Reference (Cisco WLC 5700 Series)* *Network Management Configuration Guide (Catalyst 3850 Switches) Network Management Configuration Guide (Cisco WLC 5700 Series)*
Platform-independent configuration information	*Identity Based Networking Services Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIBs

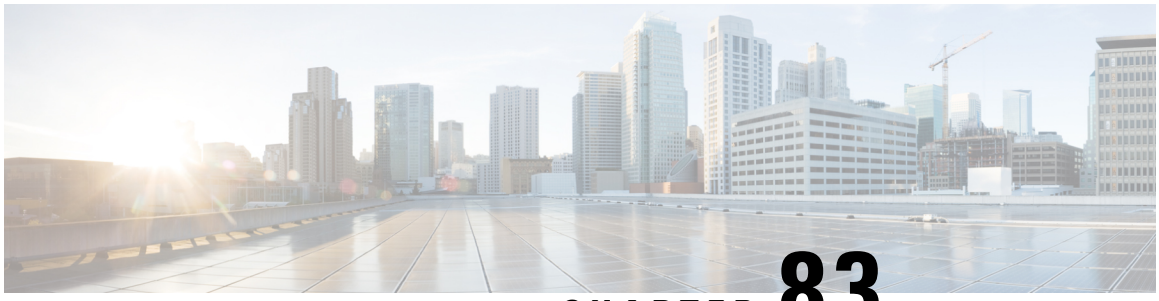
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for VLAN Groups

Release	Modification
Cisco IOS XE 3.2E	This feature was introduced
Cisco IOS XE 3.3SE	VLAN GUI support.



CHAPTER 83

Configuring VLAN Trunks

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VLAN Trunks

The IEEE 802.1Q trunks impose these limitations on the trunking strategy for a network:

- In a network of Cisco switches connected through IEEE 802.1Q trunks, the switches maintain one spanning-tree instance for each VLAN allowed on the trunks. Non-Cisco devices might support one spanning-tree instance for all VLANs.

  When you connect a Cisco switch to a non-Cisco device through an IEEE 802.1Q trunk, the Cisco switch combines the spanning-tree instance of the VLAN of the trunk with the spanning-tree instance of the non-Cisco IEEE 802.1Q switch. However, spanning-tree information for each VLAN is maintained by Cisco switches separated by a cloud of non-Cisco IEEE 802.1Q switches. The non-Cisco IEEE 802.1Q cloud separating the Cisco switches is treated as a single trunk link between the switches.

- Make sure the native VLAN for an IEEE 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.
- Disabling spanning tree on the native VLAN of an IEEE 802.1Q trunk without disabling spanning tree on every VLAN in the network can potentially cause spanning-tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an IEEE 802.1Q trunk or disable spanning tree on every VLAN in the network. Make sure your network is loop-free before disabling spanning tree.

Restrictions for VLAN Trunks

The following are restrictions for VLAN trunks:

- A trunk port cannot be a secure port.
- Trunk ports can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, the switch propagates the setting that you entered to all ports in the group:
  - Allowed-VLAN list.
  - STP port priority for each VLAN.
  - STP Port Fast setting.
  - Trunk status:

    If one port in a port group ceases to be a trunk, all ports cease to be trunks.
- We recommend that you configure no more than 24 trunk ports in Per VLAN Spanning Tree (PVST) mode and no more than 40 trunk ports in Multiple Spanning Tree (MST) mode.
- If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, the port mode is not changed.
- A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable IEEE 802.1x on a dynamic port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to dynamic, the port mode is not changed.
- Dynamic Trunking Protocol (DTP) is not supported on tunnel ports.
- The switch does not support Layer 3 trunks; you cannot configure subinterfaces or use the **encapsulation** keyword on Layer 3 interfaces. The switch does support Layer 2 trunks and Layer 3 VLAN interfaces, which provide equivalent capabilities.
- You cannot have a switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches.

Information About VLAN Trunks

Trunking Overview

A trunk is a point-to-point link between one or more Ethernet switch interfaces and another networking device such as a router or a switch. Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network.

The following trunking encapsulations are available on all Ethernet interfaces:

- IEEE 802.1Q— Industry-standard trunking encapsulation.

Trunking Modes

Ethernet trunk interfaces support different trunking modes. You can set an interface as trunking or nontrunking or to negotiate trunking with the neighboring interface. To autonegotiate trunking, the interfaces must be in the same VTP domain.

Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a Point-to-Point Protocol (PPP). However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations.

Related Topics

Configuring a Trunk Port (CLI), on page 1504
Layer 2 Interface Modes, on page 1501

Layer 2 Interface Modes

Table 121: Layer 2 Interface Modes

Mode	Function
switchport mode access	Puts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface regardless of whether or not the neighboring interface is a trunk interface.
switchport mode dynamic auto	Makes the interface able to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to **trunk** or **desirable** mode. The default switchport mode for all Ethernet interfaces is **dynamic auto**.
switchport mode dynamic desirable	Makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.
switchport mode trunk	Puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link. The interface becomes a trunk interface even if the neighboring interface is not a trunk interface.

Mode	Function
switchport nonegotiate	Prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is **access** or **trunk**. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.

Related Topics

Configuring a Trunk Port (CLI), on page 1504
Trunking Modes, on page 1501

Allowed VLANs on a Trunk

By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs, 1 to 4094, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk.

To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), DTP, and VTP in VLAN 1.

If a trunk port with VLAN 1 disabled is converted to a nontrunk port, it is added to the access VLAN. If the access VLAN is set to 1, the port will be added to VLAN 1, regardless of the **switchport trunk allowed** setting. The same is true for any VLAN that has been disabled on the port.

A trunk port can become a member of a VLAN if the VLAN is enabled, if VTP knows of the VLAN, and if the VLAN is in the allowed list for the port. When VTP detects a newly enabled VLAN and the VLAN is in the allowed list for a trunk port, the trunk port automatically becomes a member of the enabled VLAN. When VTP detects a new VLAN and the VLAN is not in the allowed list for a trunk port, the trunk port does not become a member of the new VLAN.

Related Topics

Defining the Allowed VLANs on a Trunk (CLI), on page 1506

Load Sharing on Trunk Ports

Load sharing divides the bandwidth supplied by parallel trunks connecting switches. To avoid loops, STP normally blocks all but one parallel link between switches. Using load sharing, you divide the traffic between the links according to which VLAN the traffic belongs.

You configure load sharing on trunk ports by using STP port priorities or STP path costs. For load sharing using STP port priorities, both load-sharing links must be connected to the same switch. For load sharing using STP path costs, each load-sharing link can be connected to the same switch or to two different switches.

Network Load Sharing Using STP Priorities

When two ports on the same switch form a loop, the switch uses the STP port priority to decide which port is enabled and which port is in a blocking state. You can set the priorities on a parallel trunk port so that the port carries all the traffic for a given VLAN. The trunk port with the higher priority (lower values) for a VLAN is forwarding traffic for that VLAN. The trunk port with the lower priority (higher values) for the same VLAN remains in a blocking state for that VLAN. One trunk port sends or receives all traffic for the VLAN.

Related Topics

Configuring Load Sharing Using STP Port Priorities (CLI), on page 1510

Network Load Sharing Using STP Path Cost

You can configure parallel trunks to share VLAN traffic by setting different path costs on a trunk and associating the path costs with different sets of VLANs, blocking different ports for different VLANs. The VLANs keep the traffic separate and maintain redundancy in the event of a lost link.

Related Topics

Configuring Load Sharing Using STP Path Cost (CLI), on page 1513

Feature Interactions

Trunking interacts with other features in these ways:

- A trunk port cannot be a secure port.
- Trunk ports can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, the switch propagates the setting that you entered to all ports in the group:
  - Allowed-VLAN list.
  - STP port priority for each VLAN.
  - STP Port Fast setting.
  - Trunk status:

    If one port in a port group ceases to be a trunk, all ports cease to be trunks.
- We recommend that you configure no more than 24 trunk ports in Per VLAN Spanning Tree (PVST) mode and no more than 40 trunk ports in Multiple Spanning Tree (MST) mode.
- If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, the port mode is not changed.
- A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable IEEE 802.1x on a dynamic port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to dynamic, the port mode is not changed.

How to Configure VLAN Trunks

To avoid trunking misconfigurations, configure interfaces connected to devices that do not support DTP to not forward DTP frames, that is, to turn off DTP.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.

- To enable trunking to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

Configuring an Ethernet Interface as a Trunk Port

Configuring a Trunk Port (CLI)

Because trunk ports send and receive VTP advertisements, to use VTP you must ensure that at least one trunk port is configured on the switch and that this trunk port is connected to the trunk port of a second switch. Otherwise, the switch cannot receive any VTP advertisements.

Before you begin

By default, an interface is in Layer 2 mode. The default mode for Layer 2 interfaces is **switchport mode dynamic auto**. If the neighboring interface supports trunking and is configured to allow trunking, the link is a Layer 2 trunk or, if the interface is in Layer 3 mode, it becomes a Layer 2 trunk when you enter the **switchport** interface configuration command.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/2`	Specifies the port to be configured for trunking, and enters interface configuration mode.
Step 4	**switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**} **Example:** `Switch(config-if)# switchport mode dynamic desirable`	Configures the interface as a Layer 2 trunk (required only if the interface is a Layer 2 access port or tunnel port or to specify the trunking mode). • **dynamic auto**—Sets the interface to a trunk link if the neighboring interface is set to trunk or desirable mode. This is the default.

	Command or Action	Purpose
		• **dynamic desirable**—Sets the interface to a trunk link if the neighboring interface is set to trunk, desirable, or auto mode. • **trunk**—Sets the interface in permanent trunking mode and negotiate to convert the link to a trunk link even if the neighboring interface is not a trunk interface.
Step 5	**switchport access vlan** *vlan-id* **Example:** `Switch(config-if)# switchport access vlan 200`	(Optional) Specifies the default VLAN, which is used if the interface stops trunking.
Step 6	**switchport trunk native vlan** *vlan-id* **Example:** `Switch(config-if)# switchport trunk native vlan 200`	Specifies the native VLAN for IEEE 802.1Q trunks.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 8	**show interfaces** *interface-id* **switchport** **Example:** `Switch# show interfaces gigabitethernet1/0/2 switchport`	Displays the switch port configuration of the interface in the *Administrative Mode* and the *Administrative Trunking Encapsulation* fields of the display.
Step 9	**show interfaces** *interface-id* **trunk** **Example:** `Switch# show interfaces gigabitethernet1/0/2 trunk`	Displays the trunk configuration of the interface.
Step 10	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Trunking Modes, on page 1501
Layer 2 Interface Modes, on page 1501

Defining the Allowed VLANs on a Trunk (CLI)

VLAN 1 is the default VLAN on all trunk ports in all Cisco switches, and it has previously been a requirement that VLAN 1 always be enabled on every trunk link. You can use the VLAN 1 minimization feature to disable VLAN 1 on any individual VLAN trunk link so that no user traffic (including spanning-tree advertisements) is sent or received on VLAN 1.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/1`	Specifies the port to be configured, and enters interface configuration mode.
Step 4	**switchport mode trunk** **Example:** `Switch(config-if)# switchport mode trunk`	Configures the interface as a VLAN trunk port.
Step 5	**switchport trunk allowed vlan** { *word* | **add** | **all** | **except** | **none** | **remove**} *vlan-list* **Example:** `Switch(config-if)# switchport trunk allowed vlan remove 2`	(Optional) Configures the list of VLANs allowed on the trunk. The *vlan-list* parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated VLAN parameters or in hyphen-specified ranges. All VLANs are allowed by default.

	Command or Action	Purpose
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	**show interfaces** *interface-id* **switchport** **Example:** `Switch# show interfaces gigabitethernet1/0/1 switchport`	Verifies your entries in the *Trunking VLANs Enabled* field of the display.
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Allowed VLANs on a Trunk, on page 1502

Changing the Pruning-Eligible List (CLI)

The pruning-eligible list applies only to trunk ports. Each trunk port has its own eligibility list. VTP pruning must be enabled for this procedure to take effect.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface`	Selects the trunk port for which VLANs should be pruned, and enters interface configuration mode.

	Command or Action	Purpose
	`gigabitethernet2/0/1`	
Step 4	**switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**} *vlan-list* [,*vlan* [,*vlan* [,,,]]	Configures the list of VLANs allowed to be pruned from the trunk. For explanations about using the **add**, **except**, **none**, and **remove** keywords, see the command reference for this release. Separate non-consecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Valid IDs are 2 to 1001. Extended-range VLANs (VLAN IDs 1006 to 4094) cannot be pruned. VLANs that are pruning-ineligible receive flooded traffic. The default list of VLANs allowed to be pruned contains VLANs 2 to 1001.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show interfaces** *interface-id* **switchport** **Example:** `Switch# show interfaces gigabitethernet2/0/1 switchport`	Verifies your entries in the *Pruning VLANs Enabled* field of the display.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring the Native VLAN for Untagged Traffic (CLI)

A trunk port configured with IEEE 802.1Q tagging can receive both tagged and untagged traffic. By default, the switch forwards untagged traffic in the native VLAN configured for the port. The native VLAN is VLAN 1 by default.

The native VLAN can be assigned any VLAN ID.

If a packet has a VLAN ID that is the same as the outgoing port native VLAN ID, the packet is sent untagged; otherwise, the switch sends the packet with a tag.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/2`	Defines the interface that is configured as the IEEE 802.1Q trunk, and enters interface configuration mode.
Step 4	**switchport trunk native vlan** *vlan-id* **Example:** `Switch(config-if)# switchport trunk native vlan 12`	Configures the VLAN that is sending and receiving untagged traffic on the trunk port. For *vlan-id*, the range is 1 to 4094.
Step 5	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show interfaces** *interface-id* **switchport** **Example:** `Switch# show interfaces gigabitethernet1/0/2 switchport`	Verifies your entries in the *Trunking Native Mode VLAN* field.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Trunk Ports for Load Sharing

Configuring Load Sharing Using STP Port Priorities (CLI)

These steps describe how to configure a network with load sharing using STP port priorities.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode on Switch A.
Step 3	**vtp domain** *domain-name* **Example:** `Switch(config)# vtp domain workdomain`	Configures a VTP administrative domain. The domain name can be 1 to 32 characters.
Step 4	**vtp mode server** **Example:** `Switch(config)# vtp mode server`	Configures Switch A as the VTP server.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show vtp status** **Example:** `Switch# show vtp status`	Verifies the VTP configuration on both Switch A and Switch B. In the display, check the *VTP Operating Mode* and the *VTP Domain Name* fields.
Step 7	**show vlan** **Example:** `Switch# show vlan`	Verifies that the VLANs exist in the database on Switch A.

	Command or Action	Purpose
Step 8	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 9	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/1`	Defines the interface to be configured as a trunk, and enters interface configuration mode.
Step 10	**switchport mode trunk** **Example:** `Switch(config-if)# switchport mode trunk`	Configures the port as a trunk port.
Step 11	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 12	**show interfaces** *interface-id* **switchport** **Example:** `Switch# show interfaces gigabitethernet1/0/1 switchport`	Verifies the VLAN configuration.
Step 13	Repeat the above steps on Switch A for a second port in the switch.	
Step 14	Repeat the above steps on Switch B to configure the trunk ports that connect to the trunk ports configured on Switch A.	
Step 15	**show vlan** **Example:** `Switch# show vlan`	When the trunk links come up, VTP passes the VTP and VLAN information to Switch B. This command verifies that Switch B has learned the VLAN configuration.
Step 16	**configure terminal** **Example:**	Enters global configuration mode on Switch A.

	Command or Action	Purpose
	`Switch# configure terminal`	
Step 17	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/1`	Defines the interface to set the STP port priority, and enters interface configuration mode.
Step 18	**spanning-tree vlan** *vlan-range* **port-priority** *priority-value* **Example:** `Switch(config-if)# spanning-tree vlan 8-10 port-priority 16`	Assigns the port priority for the VLAN range specified. Enter a port priority value from 0 to 240. Port priority values increment by 16.
Step 19	**exit** **Example:** `Switch(config-if)# exit`	Returns to global configuration mode.
Step 20	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/2`	Defines the interface to set the STP port priority, and enters interface configuration mode.
Step 21	**spanning-tree vlan** *vlan-range* **port-priority** *priority-value* **Example:** `Switch(config-if)# spanning-tree vlan 3-6 port-priority 16`	Assigns the port priority for the VLAN range specified. Enter a port priority value from 0 to 240. Port priority values increment by 16.
Step 22	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 23	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.

	Command or Action	Purpose
Step 24	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Network Load Sharing Using STP Priorities, on page 1502

Configuring Load Sharing Using STP Path Cost (CLI)

These steps describe how to configure a network with load sharing using STP path costs.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode on Switch A.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/1`	Defines the interface to be configured as a trunk, and enters interface configuration mode.
Step 4	**switchport mode trunk** **Example:** `Switch(config-if)# switchport mode trunk`	Configures the port as a trunk port.
Step 5	**exit** **Example:** `Switch(config-if)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 6	Repeat Steps 2 through 4 on a second interface in Switch A .	
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 8	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries. In the display, make sure that the interfaces are configured as trunk ports.
Step 9	**show vlan** **Example:** `Switch# show vlan`	When the trunk links come up, Switch A receives the VTP information from the other switches. This command verifies that Switch A has learned the VLAN configuration.
Step 10	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 11	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet1/0/1`	Defines the interface on which to set the STP cost, and enters interface configuration mode.
Step 12	**spanning-tree vlan** *vlan-range* **cost** *cost-value* **Example:** `Switch(config-if)# spanning-tree vlan 2-4 cost 30`	Sets the spanning-tree path cost to 30 for VLANs 2 through 4.
Step 13	**end** **Example:** `Switch(config-if)# end`	Returns to global configuration mode.
Step 14	Repeat Steps 9 through 13 on the other configured trunk interface on Switch A, and	

	Command or Action	Purpose
	set the spanning-tree path cost to 30 for VLANs 8, 9, and 10.	
Step 15	**exit** **Example:** `Switch(config)# exit`	Returns to privileged EXEC mode.
Step 16	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries. In the display, verify that the path costs are set correctly for both trunk interfaces.
Step 17	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Network Load Sharing Using STP Path Cost, on page 1503

Where to Go Next

After configuring VLAN trunks, you can configure the following:

- VLANs
- VLAN groups

Additional References

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	*VLAN Command Reference (Catalyst 3850 Switches) VLAN Command Reference (Cisco WLC 5700 Series)* *Layer 2/3 Command Reference (Catalyst 3850 Switches)Layer 2 Command Reference (Cisco WLC 5700 Series)* *Command Reference (Catalyst 9300 Series Switches)* *Command Reference (Catalyst 9500 Series Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

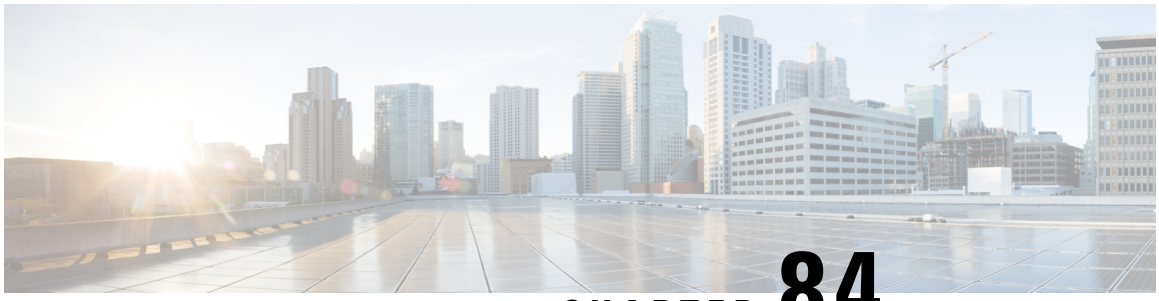
Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for VLAN Trunks

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

PART XV

WLAN



CHAPTER 84

Configuring WLANs

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About WLANs

This feature enables you to control up to WLANs for lightweight access points. Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. All switches publish up to 16 WLANs to each connected access point, but you can create up to the maximum number of WLANs supported and then selectively publish these WLANs (using access point groups) to different access points to better manage your wireless network.

You can configure WLANs with different SSIDs or with the same SSID. An SSID identifies the specific wireless network that you want the switch to access.

Band Selection

Band selection enables client radios that are capable of dual-band (2.4- and 5-GHz) operation to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of three nonoverlapping channels. To prevent these sources of interference and improve overall network performance, you can configure band selection on the switch.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 1534
Configuring Advanced WLAN Properties (GUI), on page 1537
Prerequisites for WLANs, on page 1523
Restrictions for WLANs, on page 1523

Off-Channel Scanning Defer

In deployments with certain power-save clients, you sometimes need to defer the Radio Resource Management's (RRM) normal off-channel scanning to avoid missing critical information from low-volume clients (for example, medical devices that use power-save mode and periodically send telemetry information). This feature improves the way that Quality of Service (QoS) interacts with the RRM scan defer feature.

You can use a client's Wi-Fi Multimedia (WMM) UP marking to configure the access point to defer off-channel scanning for a configurable period of time if it receives a packet marked UP.

Off-Channel Scanning Defer is essential to the operation of RRM, which gathers information about alternate channel choices such as noise and interference. Additionally, Off-Channel Scanning Defer is responsible for rogue detection. Devices that need to defer Off-Channel Scanning Defer should use the same WLAN as often as possible. If there are many of these devices (and the possibility exists that Off-Channel Defer scanning could be completely disabled by the use of this feature), you should implement an alternative to local AP Off-Channel Scanning Defer, such as monitoring access points, or other access points in the same location that do not have this WLAN assigned.

You can assign a QoS policy (bronze, silver, gold, and platinum) to a WLAN to affect how packets are marked on the downlink connection from the access point regardless of how they were received on the uplink from the client. UP=1,2 is the lowest priority, and UP=0,3 is the next higher priority. The marking results of each QoS policy are as follows:

- Bronze marks all downlink traffic to UP= 1.
- Silver marks all downlink traffic to UP= 0.
- Gold marks all downlink traffic to UP=4.
- Platinum marks all downlink traffic to UP=6.

DTIM Period

In the 802.11 networks, lightweight access points broadcast a beacon at regular intervals, which coincides with the Delivery Traffic Indication Map (DTIM). After the access point broadcasts the beacon, it transmits any buffered broadcast and multicast frames based on the value set for the DTIM period. This feature allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

Typically, the DTIM value is set to 1 (to transmit broadcast and multicast frames after every beacon) or 2 (to transmit after every other beacon). For instance, if the beacon period of the 802.11 network is 100 ms and the DTIM value is set to 1, the access point transmits buffered broadcast and multicast frames 10 times per second. If the beacon period is 100 ms and the DTIM value is set to 2, the access point transmits buffered broadcast and multicast frames 5 times per second. Either of these settings are suitable for applications, including Voice Over IP (VoIP), that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (to transmit broadcast and multicast frames after every 255th beacon) if all 802.11 clients have power save enabled. Because the clients have to listen only when the DTIM period is reached, they can be set to listen for broadcasts and multicasts less frequently which results in a longer battery life. For example, if the beacon period is 100 ms and you set the DTIM value to 100, the access point transmits buffered broadcast and multicast frames once every 10 seconds. This rate allows the power-saving clients to sleep longer before they have to wake up and listen for broadcasts and multicasts, which results in a longer battery life.

Note A beacon period, which is specified in milliseconds on the switch, is converted internally by the software to 802.11 Time Units (TUs), where 1 TU = 1.024 milliseconds. On Cisco's 802.11n access points, this value is rounded to the nearest multiple of 17 TUs. For example, a configured beacon period of 100 ms results in an actual beacon period of 104 ms.

Many applications cannot tolerate a long time between broadcast and multicast messages, which results in poor protocol and application performance. We recommend that you set a low DTIM value for 802.11 networks that support such clients.

Session Timeouts

You can configure a WLAN with a session timeout. The session timeout is the maximum time for a client session to remain active before requiring reauthorization.

Cisco Client Extensions

The Cisco Client Extensions (CCX) software is licensed to manufacturers and vendors of third-party client devices. The CCX code resident on these clients enables them to communicate wirelessly with Cisco access points and to support Cisco features that other client devices do not, including those features that are related to increased security, enhanced performance, fast roaming, and power management.

- The software supports CCX versions 1 through 5, which enables switches and their access points to communicate wirelessly with third-party client devices that support CCX. CCX support is enabled automatically for every WLAN on the switch and cannot be disabled. However, you can configure Aironet information elements (IEs).
- If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the switch sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the switch and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 1534

Configuring Advanced WLAN Properties (GUI), on page 1537
Prerequisites for WLANs, on page 1523
Restrictions for WLANs, on page 1523

Peer-to-Peer Blocking

Peer-to-peer blocking is applied to individual WLANs, and each client inherits the peer-to-peer blocking setting of the WLAN to which it is associated. Peer-to-Peer enables you to have more control over how traffic is directed. For example, you can choose to have traffic bridged locally within the switch, dropped by the switch, or forwarded to the upstream VLAN.

Peer-to-peer blocking is supported for clients that are associated with the local switching WLAN.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 1534
Configuring Advanced WLAN Properties (GUI), on page 1537
Prerequisites for WLANs, on page 1523
Restrictions for WLANs, on page 1523

Diagnostic Channel

You can choose a diagnostic channel to troubleshoot why the client is having communication problems with a WLAN. You can test the client and access points to identify the difficulties that the client is experiencing and allow corrective measures to be taken to make the client operational on the network. You can use the switch GUI or CLI to enable the diagnostic channel, and you can use the switch CLI to run the diagnostic tests.

Note We recommend that you enable the diagnostic channel feature only for nonanchored SSIDs that use the management interface. CCX Diagnostic feature has been tested only with clients having Cisco ADU card

Per-WLAN Radius Source Support

The switch sources RADIUS traffic from the IP address of its management interface unless the configured RADIUS server exists on a VLAN accessible via one of the switch Dynamic interfaces. If a RADIUS server is reachable via a switch Dynamic interface, RADIUS requests to this specific RADIUS server will be sourced from the controller via the corresponding Dynamic interface.

By default, RADIUS packets sourced from the switch will set the NAS-IP-Address attribute to that of the management interface's IP Address, regardless of the packet's source IP Address (Management or Dynamic, depending on topology).

When you enable per-WLAN RADIUS source support (Radius Server Overwrite interface) the NAS-IP-Address attribute is overwritten by the switch to reflect the sourced interface. Also, RADIUS attributes are modified accordingly to match the identity. This feature virtualizes the switch on the per-WLAN RADIUS traffic, where each WLAN can have a separate layer 3 identity. This feature is useful in deployments that integrate with ACS Network Access Restrictions and Network Access Profiles.

To filter WLANs, use the callStationID that is set by RFC 3580 to be in the APMAC:SSID format. You can also extend the filtering on the authentication server to be on a per-WLAN source interface by using the NAS-IP-Address attribute.

You can combine per-WLAN RADIUS source support with the normal RADIUS traffic source and some WLANs that use the management interface and others using the per-WLAN dynamic interface as the address source.

Prerequisites for WLANs

- You can associate up to 16 WLANs with each access point group and assign specific access points to each group. Each access point advertises only the enabled WLANs that belong to its access point group. The access point (AP) does not advertise disabled WLANs in its access point group or WLANs that belong to another group.
- We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that switches properly route VLAN traffic.

Related Topics

Creating WLANs (CLI), on page 1526
Creating WLANs (GUI), on page 1527
Configuring General WLAN Properties (CLI), on page 1531
Configuring General WLAN Properties (GUI), on page 1533
Deleting WLANs (CLI), on page 1528
Configuring Advanced WLAN Properties (CLI), on page 1534
Configuring Advanced WLAN Properties (GUI), on page 1537
Band Selection, on page 1520
DTIM Period
Session Timeout
Cisco Client Extensions, on page 1521
Peer-to-Peer Blocking, on page 1522
Diagnostic Channel
Client Count Per WLAN
Enabling WLANs (CLI), on page 1530
Disabling WLANs (CLI), on page 1530

Restrictions for WLANs

- When you change the WLAN profile name, then FlexConnect APs (using AP-specific VLAN mapping) will become WLAN-specific. If FlexConnect Groups are properly configured, the VLAN mapping will become Group-specific.
- Do not enable IEEE 802.1X Fast Transition on Flex Local Authentication enabled WLAN, as client association is not supported with Fast Transition 802.1X key management.
- Peer-to-peer blocking does not apply to multicast traffic.
- You can configure a maximum of up to 12000 clients.

- You can configure a maximum up to of 2000 clients.
- The WLAN name and SSID can have up to 32 characters.
- Special characters are not supported for the WLAN name.
- WLAN name cannot be a keyword; for example, if you try to create a WLAN with the name as 's' by entering the **wlan s** command, it results in shutting down all WLANs because 's' is used as a keyword for shutdown.
- You cannot map a WLAN to VLAN0, and you cannot map VLANs 1002 to 1006.
- Dual stack clients with a static-IPv4 address is not supported.
- When creating a WLAN with the same SSID, you must create a unique profile name for each WLAN.
- When multiple WLANs with the same SSID get assigned to the same AP radio, you must have a unique Layer 2 security policy so that clients can safely select between them.
- When AAA override is enabled on WLAN with flex local switching, the client must receive the IPv6 address from the VLAN returned by the AAA server. This implies that if a WLAN with both local switching and AAA override enabled is mapped to VLAN X and the AAA server returns a VLAN Y; then, the client must receive an address from VLAN Y. However, this is not supported in this controller release.
- When WLAN is local switching, associate the client to local-switching WLAN where AVC is enabled. Send some traffic from client, when you check the AVC stats after 90 sec. Cisco WLC shows stats under top-apps but does not show under client. There is timer issue so for the first slot Cisco WLC might not show stats for the clients. Earlier, only 1 sec stats for a client is seen if the timers at AP and at WLC are off by 89 seconds. Now, clearing of the stats is after 180 seconds so stats from 91 seconds to 179 seconds for a client is seen. This is done because two copies of the stats per client cannot be kept due to memory constraint in Cisco 5508 WLC.
- RADIUS Server Overwrite interface per wlan feature is not supported. However, you can achieve the same using the following configuration:
  - Configure a RADIUS Authentication Server
  - Configure a RADIUS Authentication Server Group
  - Create 802.1x WLAN
  - Configure Wireless Profile Policy and Attach it to the VLAN

Configure a RADIUS Authentication Server

- Device (config)# **radius server** *server-name*
- Device (config-radius-server)# **address ipv4** *address* **auth-port** *auth_port_number* **acct-port** *acct_port_number*
- Device (config-radius-server)# **key** *key*

Configure a RADIUS Authentication Server Group

- Device(config)# **aaa group server radius** *server-name*
- Device(config)# **server name** *server-name*

- Device(config)# **ip radius source-interface vlan** *vlan-name*
- Device(config)# **aaa authentication dot1x** *dot1x_name* **group** *server-name*

Create 802.1x WLAN

- Device(config)# **wlan** *wlan-name id ssid*
- Device(config-wlan)# **security dot1x authentication-list** *list-name*
- Device(config-wlan)# **no shutdown**

Configure Wireless Profile Policy and Attach it to VLAN

- Device(config)# **wireless profile policy** *profile-name*
- Device(config-wireless-policy)# **vlan** *vlan-name*
- Device(config-wireless-policy)# **no shutdown**

A sample configuration on the Cisco Wireless Controller is given below:

```
radius server RAD_EXT_3

 address ipv4 9.2.62.56 auth-port 1812 acct-port 1813

 key cisco


aaa group server radius AAA_EXT_3
server name RAD_EXT_3
ip radius source-interface vlan 50

aaa authentication dot1x test_ext group AAA_EXT_3

wlan test_wpa2_dot1x 2 test_wpa2_dot1x
security dot1x authentication-list test_ext
no shutdown


wireless profile policy pp-1
vlan 50
no shutdown


radius server RAD_EXT_3

 address ipv4 9.2.62.56 auth-port 1812 acct-port 1813

 key cisco


aaa group server radius AAA_EXT_2
server name RAD_EXT_3
ip radius source-interface vlan 51

aaa authentication dot1x test_ext_2 group AAA_EXT_2

wlan test_wpa2 3 test_wpa3
security dot1x authentication-list test_ext_2
no shutdown
```

```
wireless profile policy pp-1
vlan 51
no shutdown
```

Caution Some clients might not be able to connect to WLANs properly if they detect the same SSID with multiple security policies. Use this feature with care.

Related Topics

Creating WLANs (CLI), on page 1526
Creating WLANs (GUI), on page 1527
Configuring General WLAN Properties (CLI), on page 1531
Configuring General WLAN Properties (GUI), on page 1533
Deleting WLANs (CLI), on page 1528
Configuring Advanced WLAN Properties (CLI), on page 1534
Configuring Advanced WLAN Properties (GUI), on page 1537
Band Selection, on page 1520
DTIM Period
Session Timeout
Cisco Client Extensions, on page 1521
Peer-to-Peer Blocking, on page 1522
Diagnostic Channel
Client Count Per WLAN
Enabling WLANs (CLI), on page 1530
Disabling WLANs (CLI), on page 1530

How to Configure WLANs

Creating WLANs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id* [*ssid*] **Example:** `Switch(config)# wlan mywlan 34 mywlan-ssid`	Specifies the WLAN name and ID: • For the *profile-name*, enter the profile name. The range is from 1 to 32 alphanumeric characters. • For the *wlan-id*, enter the WLAN ID. The range is from 1 to 512.

	Command or Action	Purpose
		• For the *ssid*, enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID. **Note** By default, the WLAN is disabled.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for WLANs, on page 1523
Restrictions for WLANs, on page 1523

Creating WLANs (GUI)

Procedure

Step 1 Click **Configuration** > **Wireless**.

The **WLANs** page is displayed.

Step 2 Click **New** to create a WLAN.

The **WLANs** > **Create New** page is displayed.

Step 3 Enter the following parameters:

Parameter	Description
WLAN ID	WLAN identifier. The value ranges from 1 to 512.
SSID	Broadcast name of the WLAN.
Profile	WLAN profile name.

Step 4 Click **Apply**.

Related Topics

Prerequisites for WLANs, on page 1523
Restrictions for WLANs, on page 1523

Deleting WLANs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**no wlan** *wlan-name wlan-id ssid* **Example:** `Switch(config)# no wlan test2`	Deletes the WLAN. The arguments are as follows: • The *wlan-name* is the WLAN profile name. • The *wlan-id* is the WLAN ID. • The *ssid* is the WLAN SSID name configured for the WLAN. **Note** If you delete a WLAN that is part of an AP group, the WLAN is removed from the AP group and from the AP's radio.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for WLANs, on page 1523
Restrictions for WLANs, on page 1523

Deleting WLANs (GUI)

Procedure

Step 1 Click **Configuration** > **Wireless**.

The **WLANs** page is displayed.

Step 2 Select the checkbox corresponding to the WLAN you want to delete.

Note If you delete a WLAN that is part of an AP group, the WLAN is removed from the AP group and from the AP's radio.

Step 3 Click **Remove**.

Searching WLANs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**show wlan summary** **Example:** `Switch# show wlan summary`	Displays the list of all WLANs configured on the device. You can search for the WLAN in the output.

Example

```
Switch# show wlan summary
Number of WLANs: 4

WLAN Profile Name                    SSID                           VLAN Status
-------------------------------------------------------------------------------
1    test1                            test1-ssid                     137  UP
3    test2                            test2-ssid                     136  UP
2    test3                            test3-ssid                     1    UP
45   test4                            test4-ssid                     1    DOWN
```

You can also use wild cards to search WLANs. For example **show wlan summary include** | *variable*. Where variable is any search string in the output.

```
Switch# show wlan summary | include test-wlan-ssid
1    test-wlan                      test-wlan-ssid                   137   UP
```

Searching WLANs (GUI)

Procedure

Step 1 Click **Configuration** > **Wireless**.

The **WLANs** page is displayed.

Step 2 Type the first few characters in the text box above the column you are searching. Fo For example, to search the WLAN based on the **Profile**, type the first few characters of the profile name.

You can search a WLAN based on the following criteria:

- **Profile**
- **ID**
- **SSID**
- **VLAN**

- **Status**

If a WLAN exists, it would appear based on the accuracy of the match.

Enabling WLANs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Enables the WLAN.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for WLANs, on page 1523
Restrictions for WLANs, on page 1523

Disabling WLANs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.

	Command or Action	Purpose
Step 3	**shutdown** **Example:** `Switch(config-wlan)# shutdown`	Disables the WLAN.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**show wlan summary** **Example:** `Switch# show wlan summary`	Displays the list of all WLANs configured on the device. You can search for the WLAN in the output.

Related Topics

Prerequisites for WLANs, on page 1523
Restrictions for WLANs, on page 1523

Configuring General WLAN Properties (CLI)

You can configure the following properties:

- Media stream
- Broadcast SSID
- Call Snooping
- Radio
- Interface
- Status

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**shutdown** **Example:** `Switch# shutdown`	Disables the WLAN before configuring the parameters.

	Command or Action	Purpose
Step 4	**broadcast-ssid** **Example:** `Switch(config-wlan)# broadcast-ssid`	Broadcasts the SSID for this WLAN. This field is enabled by default.
Step 5	**radio** {**all** | **dot11a** | **dot11ag** | **dot11bg** | **dot11g**} **Example:** `Switch# radio all`	Enables radios on the WLAN. The keywords are as follows: • **all**—Configures the WLAN on all radio bands. • **dot1a**—Configures the WLAN on only 802.11a radio bands. • **dot11g**—Configures the WLAN on 802.11ag radio bands. • **dot11bg**—Configures the WLAN on only 802.11b/g radio bands (only 802.11b if 802.11g is disabled). • **dot11ag**— Configures the wireless LAN on 802.11g radio bands only.
Step 6	**client vlan** *vlan-identifier* **Example:** `Switch# client vlan test-vlan`	Enables an interface group on the WLAN. *vlan-identifier*—Specifies the VLAN identifier. This can be the VLAN name, VLAN ID, or VLAN group name.
Step 7	**ip multicast vlan** *vlan-name* **Example:** `Switch(config-wlan)# ip multicast vlan test`	Enables IP multicast on a WLAN. The keywords are as follows: • **vlan**—Specifies the VLAN ID. • *vlan-name*—Specifies the VLAN name.
Step 8	**media-stream multicast-direct** **Example:** `Switch(config-wlan)# media-stream multicast-direct`	Enables multicast VLANs on this WLAN.
Step 9	**call-snoop** **Example:** `Switch(config-wlan)# call-snoop`	Enables call-snooping support.
Step 10	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Enables the WLAN.

	Command or Action	Purpose
Step 11	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for WLANs, on page 1523
Restrictions for WLANs, on page 1523

Configuring General WLAN Properties (GUI)

Use this procedure to perform the following actions on a WLAN:

- Set WLAN Status
- Configure Radio Policies
- Assign Interface/Interface Groups
- Enable or Disable Multicast VLAN Feature
- Enable or Disable Broadcast SSID Feature

Procedure

Step 1 Click **Configuration** > **Wireless**.

The **WLANs** page is displayed.

Step 2 Locate the WLAN you want to configure by using the search mechanisms on the page.

Step 3 Click on the **WLAN Profile** of the WLAN.

The **WLAN** > **Edit** page is displayed.

Step 4 Click the **General** tab. This tab is displayed by default.

Step 5 Configure the **General** parameters.

Parameter	Description
Profile Name	Displays the configured profile name of the WLAN.
Type	Displays the configured LAN type.
SSID	Displays the configured SSID of the WLAN.
Status	Check box to enable the WLAN. The default value is enabled.
Security Policies	WLAN security policies set using the Security tab.

Parameter	Description
Radio Policy	WLAN radio policy to enable radios on the WLAN. Values are the following: • All • 802.11a only • 802.11g only • 802.11a/g only • 802.11b/g only
Interface/Interface Group	Interface or interface group that you want this WLAN to be mapped. Displays the non-service port and non-virtual interface names configured on the **Interfaces** page. **Note** This field displays a drop down box only when the VLAN for a WLAN is mapped using a existing VLAN name on the switch.
Broadcast SSID	Check box to broadcast this SSID. The default is enabled.
Multicast VLAN Feature	Check box to enable the multicast VLAN. The default is disabled. **Note** The Multicast Interface field appears only after you enable the Multicast VLAN feature text box. **Note** You have to configure the multicast VLAN feature only once if you want to use the multicast feature.

Step 6 Click **Apply**.

What to do next

Proceed to configure the Security, QoS, and Advanced Properties.

Related Topics

Prerequisites for WLANs, on page 1523
Restrictions for WLANs, on page 1523

Configuring Advanced WLAN Properties (CLI)

You can configure the following advanced properties:

- AAA Override
- Coverage Hole Detection
- Session Timeout
- Cisco Client Extensions
- Diagnostic Channels
- Interface Override ACLs

- P2P Blocking
- Client Exclusion
- Maximum Clients Per WLAN
- Off Channel Scan Defer

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**aaa-override** **Example:** `Switch(config-wlan)# aaa-override`	Enables AAA override.
Step 4	**chd** **Example:** `Switch(config-wlan)# chd`	Enables coverage hole detection for this WLAN. This field is enabled by default.
Step 5	**session-timeout** *time-in-seconds* **Example:** `Switch(config-wlan)# session-timeout 450`	Sets the session timeout in seconds. The range and default values vary according to the security configuration. If the WLAN security is configured to dot1x, the range is 300 to 86400 seconds and the default value is 1800 seconds. For all other WLAN security configurations, the range is 1 to 65535 seconds and the default value is 0 seconds. A value of 0 indicates no session timeout.
Step 6	**ccx aironet-iesupport** **Example:** `Switch(config-wlan)# ccx aironet-iesupport`	Enables support for Aironet IEs for this WLAN. This field is enabled by default.
Step 7	**diag-channel** **Example:** `Switch(config-wlan)# diag-channel`	Enables diagnostic channel support to troubleshoot client communication issues on a WLAN.
Step 8	**ip access-group** [web] *acl-name* **Example:**	Configures the WLAN ACL group. The variable *acl-name* specifies the user-defined

	Command or Action	Purpose
	`Switch(config)# ip access-group test-acl-name`	IPv4 ACL name. The keyword **web** specifies the IPv4 web ACL.
Step 9	**peer-blocking** [**drop** | **forward-upstream**] **Example:** `Switch(config)# peer-blocking drop`	Configures peer to peer blocking parameters. The keywords are as follows: • **drop**—Enables peer-to-peer blocking on the drop action. • **forward-upstream**—Enables peer-to-peer blocking on the forward upstream action.
Step 10	**exclusionlist** *time-in-seconds* **Example:** `Switch(config)# exclusionlist 10`	Specifies the timeout in seconds. The valid range is from 0 to 2147483647. Enter 0 for no timeout. A zero (0) timeout indicates that the client is permanently added to the exclusion list.
Step 11	**client association limit** *max-number-of-clients* **Example:** `Switch(config)# client association limit 200`	Sets the maximum number of clients that can be configured on a WLAN.
Step 12	**channel-scan defer-priority** {**defer-priority** {**0-7**} | **defer-time** {**0 - 6000**}} **Example:** `Switch(config)# channel-scan defer-priority 6`	Sets the channel scan defer priority and defer time. The arguments are as follows: • **defer-priority**—Specifies the priority markings for packets that can defer off-channel scanning. The range is from 0 to 7. The default is 3. • **defer-time**—Deferral time in milliseconds. The range is from 0 to 6000. The default is 100.
Step 13	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Band Selection, on page 1520
DTIM Period
Session Timeout
Cisco Client Extensions, on page 1521
Peer-to-Peer Blocking, on page 1522
Diagnostic Channel
Client Count Per WLAN
Prerequisites for WLANs, on page 1523

Restrictions for WLANs, on page 1523
Information About AAA Override, on page 1556
Prerequisites for Layer 2 Security, on page 1555

Configuring Advanced WLAN Properties (GUI)

Procedure

Step 1 Click **Configuration** > **Wireless**.

The **WLANs** page is displayed.

Step 2 Locate the WLAN you want to configure by using the search mechanisms on the page.

Step 3 Click on the **WLAN Profile** of the WLAN.

The **WLAN** > **Edit** page is displayed.

Step 4 Click on the **Advanced Properties** tab.

Step 5 Configure the **Advanced** properties.

Parameter	Description
Allow AAA Override	AAA override for global WLAN parameters that you can enable or disable. When AAA Override is enabled, and a client has conflicting AAA and switches WLAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the operating system moves clients from the default Cisco WLAN Solution WLAN VLAN to a VLAN returned by the AAA server and predefined in the switches interface configuration. In all cases, the operating system also uses QoS, DSCP, 802.1p priority tag values, and ACLs provided by the AAA server, if they are predefined in the switches interface configuration. (This VLAN switching by AAA Override is also referred to as Identity Networking.) If the Corporate WLAN primarily uses a Management Interface assigned to VLAN 2, and if AAA Override returns a redirect to VLAN 100, the operating system redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned. When AAA Override is disabled, all client authentication defaults to the switches authentication parameter settings, and authentication is performed only by the AAA server if the switches WLAN does not contain any client-specific authentication parameters. The AAA override values might come from a RADIUS server, for example.

Parameter	Description
Coverage Hole Detection	Coverage hole detection (CHD) on this WLAN that you can enable or disable. By default, CHD is enabled on all WLANs on the switches. You can disable CHD on a WLAN. When you disable CHD on a WLAN, a coverage hole alert is still sent to the Switch, but no other processing is done to mitigate the coverage hole. This feature is useful for guest WLANs where guests are connected to your network for short periods of time and are likely to be highly mobile.
Session Timeout	Configure a WLAN with a session timeout in seconds. The session timeout is the maximum time for a client session to remain active before requiring reauthorization. The minimum session timeout allowed is 1 second and the maximum timeout allowed is 65535 seconds. **Note** Entering zero denotes the session will never expire.
Aironet IE	Support of Aironet IEs per WLAN that you can enable or disable. The default is disabled.
Diagnostic Channel	Diagnostic channel support on the WLAN that you can enable or disable. The default is disabled.
P2P Blocking Action	Peer-to-peer blocking settings that you can choose from the following: • Disabled—(Default) Disables peer-to-peer blocking and bridges traffic locally within the switch whenever possible. • Drop—Causes the switches to discard the packets. • Forward-UpStream—Causes the packets to be forwarded on the upstream VLAN. The device above the switches decides what action to take regarding the packets.
Client Exclusion	Timeout in seconds for disabled client machines that you can enable or disable. Client machines are disabled by their MAC address and their status can be observed on the Clients > Details page. A timeout setting of 0 indicates that the client is disabled permanently. Administrative control is required to reenable the client. The default is enabled and the timeout setting is configured as 60 seconds.
Timeout Value (secs)	The minimum timeout value allowed is 0 seconds and the maximum timeout value allowed is 2147483647 seconds.
Max Allowed Client	Maximum clients allowed per Switch. You can set a limit to the number of clients that can connect to a WLAN. This feature is useful in scenarios where you have a limited number of clients that can connect to a Switch. You can set a limit on the number of guest clients that can access a given WLAN. The number of clients that you can configure per WLAN depends on the platform that you are using. A maximum of up to 12000 clients are supported. **Note** The maximum number of clients per WLAN feature is supported only for access points that are in connected mode.
DHCP	

Parameter	Description
DHCP Server IP Address	Enter the DHCP server on the WLAN that overrides the DHCP server address on the interface assigned to the WLAN.
DHCP Address Assignment Required	Enables the DHCP address assignment and makes it mandatory for clients to get their IP address from the DHCP server.
DHCP Option 82	Enables the DHCP82 payload on the WLAN.
DHCP option 82 Format	Specifies the DHCP option 82 format. Values are as follows: • add-ssid— Set RemoteID format that is the AP radio MAC address and SSID. • ap-ethmac—Set RemoteID format that is the AP Ethernet MAC address. **Note** If the format option is not configured, only the AP radio MAC address is used.
DHCP Option ASCII Mode	Configures ASCII for DHCP Option 82. If this is not configured, the option 82 format is set to ASCII format.
DHCP Option 82 RID Mode	Adds the Cisco 2 Byte RID for DHCP option 82.
NAC	
NAC State	Enables the NAC on the WLAN.
Off Channel Scanning Defer	
Scan Differ Priority	Defer priority for the channel scan that you can assign by clicking on the priority argument. The valid range for the priority is 0 to 7. The priority is 0 to 7 (this value should be set to 6 on the client and on the WLAN). Multiple values can be set. The default values are 4, 5 and 6.
Scan Differ Time	Channel scan defer time in milliseconds that you can assign. The valid range is 100 (default) to 60000 (60 seconds). This setting should match the requirements of the equipment on your wireless LAN.
Override Interface ACL	
IPv4 ACL	The WLANs IPv4 ACL group. Values are as follows: • Un-configured • Pre-auth_ipv4_acl
IPv6 ACL	The WLANs IPv6 ACL group. Values are as follows: • Un-configured • Pre-auth_ipv6_acl

Step 6 Click **Apply**.

Related Topics

Band Selection, on page 1520

Applying a QoS Policy on a WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless**.

Step 2 Expand the **WLAN** node by clicking on the left pane and choose **WLANs**.

The **WLANs** page is displayed.

Step 3 Select the WLAN for which you want to configure the QoS policies by clicking on the WLAN **Profile**.

Step 4 Click the QoS tab to configure the QoS policies on the WLAN.

You can also configure precious metal policies for the WLAN.

The following options are available:

Parameter	Description
QoS SSID Policy	
Egress Policy	QoS downstream policy configuration. The **Existing Policy** column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the **Assign Policy** column. If a policy is not selected, NONE is displayed.
Ingress Policy	QoS upstream policy configuration. The **Existing Policy** column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the **Assign Policy** column. If a policy is not selected, NONE is displayed.
QoS Client Policy	
Egress Policy	QoS downstream policy configuration. The **Existing Policy** column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the **Assign Policy** column. If a policy is not selected, NONE is displayed.

Parameter	Description
Ingress Policy	QoS upstream policy configuration. The **Existing Policy** column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the **Assign Policy** column. If a policy is not selected, NONE is displayed.
WMM	
WMM Policy	WMM Policy. This parameter has the following values: • Disabled—Disables this WMM policy. • Allowed—Allows the clients to communicate with the WLAN. • Require—Ensures that it is mandatory for the clients to have WMM features enabled on them to communicate with the WLAN.

Step 5 Click **Apply**.

Related Topics

Port Policies, on page 596
Port Policy Format, on page 596
Restrictions for QoS on Wireless Targets, on page 632
Supported QoS Features on Wireless Targets, on page 594
Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic, on page 696
SSID Policies, on page 598
Examples: SSID Policy
Examples: Configuring Downstream SSID Policy, on page 697
Client Policies, on page 599
Examples: Client Policies, on page 699

Monitoring WLAN Properties (CLI)

Command	Description
show wlan id *wlan-id*	Displays WLAN properties based on the WLAN ID.
show wlan name *wlan-name*	Displays WLAN properties based on the WLAN name.
show wlan all	Displays WLAN properties of all configured WLANs.

Command	Description
show wlan summary	Displays a summary of all WLANs. The summary details includes the following information: • WLAN ID • Profile name • SSID • VLAN • Status
show running-config wlan *wlan-name*	Displays the running configuration of a WLAN based on the WLAN name.
show running-config *wlan*	Displays the running configuration of all WLANs.

Viewing WLAN Properties (GUI)

Before you begin

- You must have administrator privileges.

Procedure

Step 1 Select **Configuration** > **WLAN**

The WLANs page is displayed.

Step 2 Click the **WLAN Profile** link.

The **WLANs** > **Edit** page is displayed. The WLANs page contains the following tabs:

- General : Displays the WLAN general properties.
- Security: Displays the security properties. The properties include Layer 2, Layer 3, and AAA properties.
- QoS: Displays the QoS configuration properties.
- Advanced: Displays the advanced properties.

Where to Go Next

Proceed to configure DHCP for WLANs.

Additional References

Related Documents

Related Topic	Document Title
WLAN command reference	*WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
Mobility Anchor configuration	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
WebAuth Configuration	*Security Configuration Guide (Catalyst 3850 Switches)Security Configuration Guide (Cisco WLC 5700 Series)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

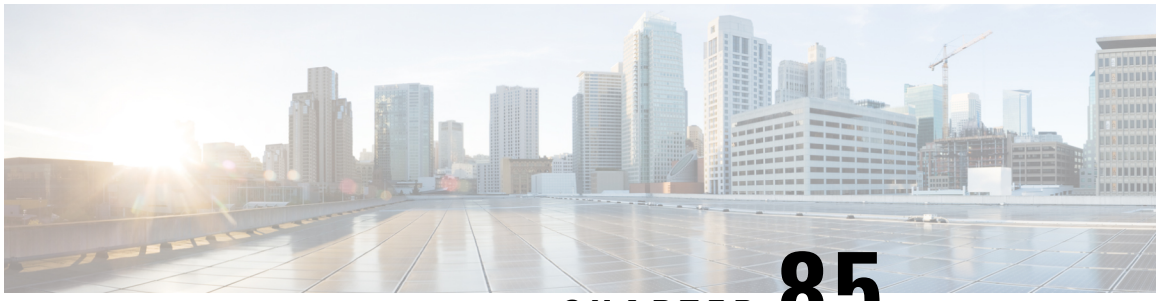
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for WLANs

This table lists the features in this module and provides links to specific configuration information:

Feature	Release	Modification
WLAN Functionality	Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 85

Configuring DHCP for WLANs

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring DHCP for WLANs

- To be able to use the DHCP option 82, you must configure DHCP on Cisco IOS software. By default, DHCP option 82 is enabled for all clients. You can control the wireless client behavior using the WLAN suboptions.
- The Cisco converged access platforms support internal DHCP server functionality. However, as a general deployment guideline to build large enterprise-class networks, we recommend that you use external DHCP server to provide dynamic IP addressing to wireless clients. Such distributed function reduces processing and configuration load on network devices and allows them to operate efficiently in large scale deployments.
- DHCP Snooping Configuration—DHCP snooping configuration is the required best practices configuration on switch for rapid client join function. DHCP snooping needs to be enabled on each client VLAN including the override VLAN if override is applied on the WLAN.

  Example of DHCP snooping configuration

1. Global DHCP snooping configuration:
   1. `Switch(config)#ip dhcp snooping`

      `Switch(config)#ip dhcp snooping vlan 100`
   2. Enable `bootp-broadcast` command. This is required for clients that send DHCP messages with broadcast addresses and broadcast bit is set in the DHCP message:

      `Switch(config)#ip dhcp snooping wireless bootp-broadcast enable`
   3. To not append DHCP Option information, enter this command:

      `Switch(config)#no ip dhcp snooping information option`
2. On the interface:

Note IP DHCP snooping trust is required on Port-Channel interface in addition to member link of the Port-Channel interface.

```
Switch(config)#interface range TenGigabitEthernet 1/0/1 - 2
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 100
Switch(config-if)#ip dhcp snooping trust


Switch(config)#interface port-channel 1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 100
Switch(config-if)#ip dhcp snooping trust
```

Note DHCP snooping must be configured on the Guest Anchor switch for guest access similar to the Config above.

Related Topics

Configuring DHCP for WLANs (CLI), on page 1551
Information About the Dynamic Host Configuration Protocol, on page 1547
Internal DHCP Servers, on page 1547
External DHCP Servers, on page 1548
DHCP Assignments, on page 1548
Information About DHCP Option 82, on page 1549
Configuring DHCP Scopes, on page 1550
Information About Internal DHCP Server, on page 1550

Restrictions for Configuring DHCP for WLANs

- If you override the DHCP server in a WLAN, you must ensure that you configure the underlying Cisco IOS configuration to make sure that the DHCP server is reachable.
- WLAN DHCP override works only if DHCP service is enabled on the switch.

  You can configure DHCP service in the following ways:

  - Configuring the DHCP pool on the switch.
  - Configuring a DHCP relay agent on the SVI. Note: the VLAN of the SVI must be mapped to the WLAN where DHCP override is configured.

Related Topics

Configuring DHCP for WLANs (CLI), on page 1551
Information About the Dynamic Host Configuration Protocol, on page 1547
Internal DHCP Servers, on page 1547
External DHCP Servers, on page 1548
DHCP Assignments, on page 1548
Information About DHCP Option 82, on page 1549
Configuring DHCP Scopes, on page 1550
Information About Internal DHCP Server, on page 1550

Information About the Dynamic Host Configuration Protocol

You can configure WLANs to use the same or different Dynamic Host Configuration Protocol (DHCP) servers or no DHCP server. Two types of DHCP servers are available: internal and external.

Related Topics

Configuring DHCP for WLANs (CLI), on page 1551
Prerequisites for Configuring DHCP for WLANs, on page 1545
Restrictions for Configuring DHCP for WLANs, on page 1547

Internal DHCP Servers

The switches contain an internal DHCP server. This server is typically used in branch offices that do not already have a DHCP server. The wireless network generally contains a maximum of 10 access points or fewer, with the access points on the same IP subnet as the switch. The internal server provides DHCP addresses to wireless clients, direct-connect access points, and DHCP requests that are relayed from access points. Only lightweight access points are supported. When you want to use the internal DHCP server, you must set the management interface IP address of the switch as the DHCP server IP address.

DHCP option 43 is not supported on the internal server. Therefore, the access point must use an alternative method to locate the management interface IP address of the switch, such as local subnet broadcast, Domain Name System (DNS), or priming.

An internal DHCP server pool only serves the wireless clients of that switch, not clients of other switches. Also, an internal DHCP server can serve only wireless clients, not wired clients.

When clients use the internal DHCP server of the switch, IP addresses are not preserved across reboots. As a result, multiple clients can be assigned with the same IP address. To resolve any IP address conflicts, clients must release their existing IP address and request a new one. Wired guest clients are always on a Layer 2 network connected to a local or foreign switch.

Note DHCPv6 is not supported in the internal DHCP servers.

Related Topics

Configuring DHCP for WLANs (CLI), on page 1551
Prerequisites for Configuring DHCP for WLANs, on page 1545
Restrictions for Configuring DHCP for WLANs, on page 1547

External DHCP Servers

The operating system is designed to appear as a DHCP Relay to the network and as a DHCP server to clients with industry-standard external DHCP servers that support DHCP Relay, which means that each switch appears as a DHCP Relay agent to the DHCP server and as a DHCP server at the virtual IP address to wireless clients.

Because the switch captures the client IP address that is obtained from a DHCP server, it maintains the same IP address for that client during intra switch, inter switch, and inter-subnet client roaming.

Note External DHCP servers can support DHCPv6.

Related Topics

Configuring DHCP for WLANs (CLI), on page 1551
Prerequisites for Configuring DHCP for WLANs, on page 1545
Restrictions for Configuring DHCP for WLANs, on page 1547

DHCP Assignments

You can configure DHCP on a per-interface or per-WLAN basis. We recommend that you use the primary DHCP server address that is assigned to a particular interface.

You can assign DHCP servers for individual interfaces. You can configure the management interface, AP-manager interface, and dynamic interface for a primary and secondary DHCP server, and you can configure the service-port interface to enable or disable DHCP servers. You can also define a DHCP server on a WLAN. In this case, the server overrides the DHCP server address on the interface assigned to the WLAN.

Security Considerations

For enhanced security, we recommend that you require all clients to obtain their IP addresses from a DHCP server. To enforce this requirement, you can configure all WLANs with a DHCP Addr. Assignment Required setting, which disallows client static IP addresses. If DHCP Addr. Assignment Required is selected, clients must obtain an IP address via DHCP. Any client with a static IP address is not allowed on the network. The switch monitors DHCP traffic because it acts as a DHCP proxy for the clients.

Note

- WLANs that support management over wireless must allow management (device-servicing) clients to obtain an IP address from a DHCP server.

If slightly less security is tolerable, you can create WLANs with DHCP Addr. Assignment Required disabled. Clients then have the option of using a static IP address or obtaining an IP address from a designated DHCP server.

Note DHCP Addr. Assignment Required is not supported for wired guest LANs.

You can create separate WLANs with DHCP Addr. Assignment Required configured as disabled. This is applicable only if DHCP proxy is enabled for the switch. You must not define the primary/secondary configuration DHCP server you should disable the DHCP proxy. These WLANs drop all DHCP requests and force clients to use a static IP address. These WLANs do not support management over wireless connections.

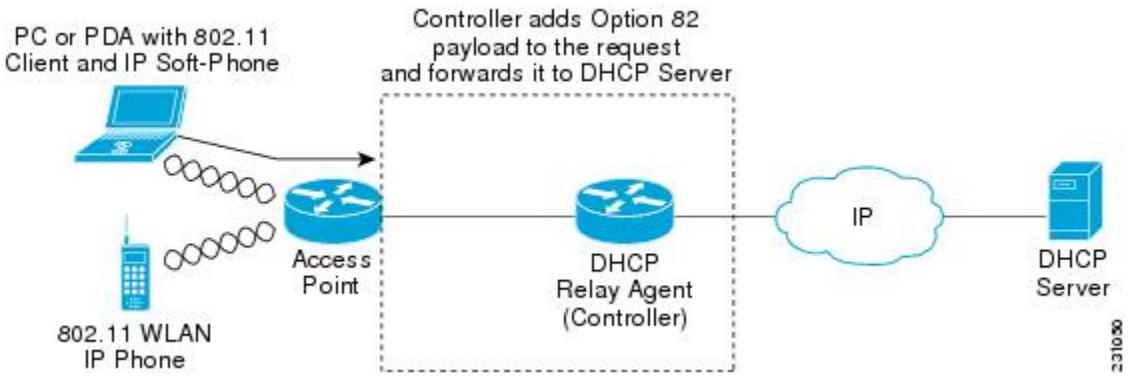
Related Topics

Configuring DHCP for WLANs (CLI), on page 1551
Prerequisites for Configuring DHCP for WLANs, on page 1545
Restrictions for Configuring DHCP for WLANs, on page 1547

Information About DHCP Option 82

DHCP option 82 provides additional security when DHCP is used to allocate network addresses. It enables the switch to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources. You can configure the switch to add option 82 information to DHCP requests from clients before forwarding the requests to the DHCP server.

Figure 74: DHCP Option 82



The access point forwards all DHCP requests from a client to the switch. The switch adds the DHCP option 82 payload and forwards the request to the DHCP server. The payload can contain the MAC address or the MAC address and SSID of the access point, depending on how you configure this option.

Note Any DHCP packets that already include a relay agent option are dropped at the switch.

For DHCP option 82 to operate correctly, DHCP proxy must be enabled.

Related Topics

Configuring DHCP for WLANs (CLI), on page 1551
Prerequisites for Configuring DHCP for WLANs, on page 1545
Restrictions for Configuring DHCP for WLANs, on page 1547

Configuring DHCP Scopes

Related Topics

Configuring DHCP for WLANs (CLI), on page 1551
Prerequisites for Configuring DHCP for WLANs, on page 1545
Restrictions for Configuring DHCP for WLANs, on page 1547

Information About Internal DHCP Server

Switches have built-in DHCP relay agents. However, when you desire network segments that do not have a separate DHCP server, the switches can have built-in internal DHCP server that assign IP addresses and subnet masks to wireless clients. Typically, one switch can have one or more internal DHCP server that each provide a range of IP addresses.

Internal DHCP server are needed for internal DHCP to work. Once DHCP is defined on the switch, you can then point the primary DHCP server IP address on the management, AP-manager, and dynamic interfaces to the switch's management interface.

Note The controller has the ability to provide internal DHCP server. This feature is very limited and considered as convenience that is often used simple demonstration or proof-of-concept, for example in a lab environment. The best practice is NOT to use this feature in an enterprise production network.

Read more about this at: http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/110865-dhcp-wlc.html#anc16

Related Topics

Configuring DHCP for WLANs (CLI), on page 1551
Prerequisites for Configuring DHCP for WLANs, on page 1545
Restrictions for Configuring DHCP for WLANs, on page 1547
Configuring DHCP Scopes (CLI), on page 1553

How to Configure DHCP for WLANs

Configuring DHCP for WLANs (CLI)

Use this procedure to configure the following DHCP parameters on a WLAN:

- DHCP Option 82 Payload
- DHCP Required
- DHCP Override

Before you begin

- You must have admin privileges for configuring the WLAN.
- To configure the DHCP override, you must have the IP address of the DHCP server.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**shutdown** **Example:** `Switch(config)# shutdown`	Shut down the WLAN.
Step 3	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 4	**ip dhcp opt82** {**ascii** | **format** {*add-ssid* | *ap-ethmac*} | **rid**} **Example:** `Switch(config)# ip dhcp opt82 format add-ssid`	Specifies the DHCP82 payload on the WLAN. The keyword and arguments are as follows: • **ascii**—Configures ASCII for DHCP Option 82. If this is not configured, the option 82 format is set to ASCII format. • **format**—Specifies the DHCP option 82 format. The following options are available: • *add-ssid*—Set RemoteID format that is the AP radio MAC address and SSID.

	Command or Action	Purpose
		• *ap-ethmac*—Set RemoteID format that is the AP Ethernet MAC address. **Note** If the format option is not configured, only the AP radio MAC address is used. • **rid**—Adds the Cisco 2 byte RID for DHCP option 82.
Step 5	**ip dhcp required** **Example:** `Switch(config-wlan)# ip dhcp required`	Makes it mandatory for clients to get their IP address from the DHCP server. Static clients are not allowed.
Step 6	**ip dhcp server** *ip-address* **Example:** `Switch(config-wlan)# ip dhcp server 200.1.1.2`	Defines a DHCP server on the WLAN that overrides the DHCP server address on the interface assigned to the WLAN.
Step 7	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Restarts the WLAN.
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 9	**show wlan** *wlan-name* **Example:** `Switch(config-wlan)# show wlan test-wlan`	Verifies the DHCP configuration.

Related Topics

Information About the Dynamic Host Configuration Protocol, on page 1547
Internal DHCP Servers, on page 1547
External DHCP Servers, on page 1548
DHCP Assignments, on page 1548
Information About DHCP Option 82, on page 1549
Configuring DHCP Scopes, on page 1550
Information About Internal DHCP Server, on page 1550
Prerequisites for Configuring DHCP for WLANs, on page 1545
Restrictions for Configuring DHCP for WLANs, on page 1547

Configuring DHCP Scopes (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ip dhcp pool** *pool-name* **Example:** `Switch(config)#ip dhcp pool test-pool`	Configures the DHCP pool address.
Step 3	**network** *network-name mask-address* **Example:** `Switch(dhcp-config)#network 209.165.200.224 255.255.255.0`	Specifies the network number in dotted-decimal notation and the mask address.
Step 4	**dns-server** *hostname* **Example:** `Switch(dhcp-config)#dns-server example.com`	Specifies the DNS name server. You can specify an IP address or a hostname.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Information About Internal DHCP Server, on page 1550

Additional References

Related Documents

Related Topic	Document Title
System Management	*System Management Configuration Guide (Catalyst 3850 Switches)System Management Configuration Guide (Cisco WLC 5700 Series)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

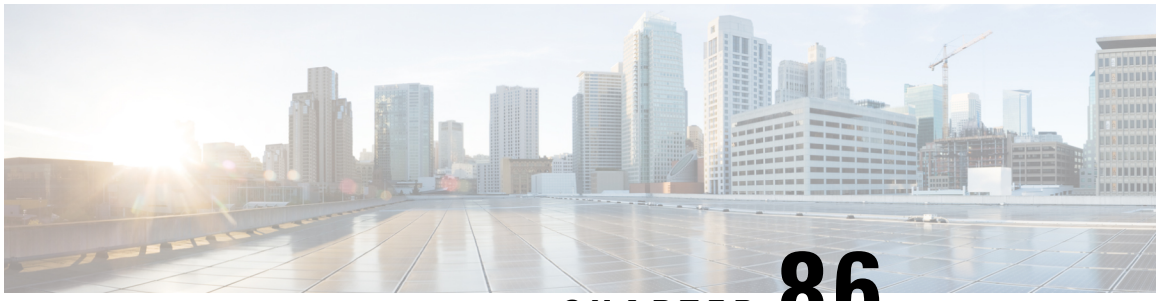
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for DHCP for WLANs

Feature Name	Release	Feature Information
DHCP functionality for WLAN	Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 86

Configuring WLAN Security

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Layer 2 Security

WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on the information advertised in beacon and probe responses. The available Layer 2 security policies are as follows:

- None (open WLAN)
- Static WEP or 802.1X

Note

- Because static WEP and 802.1X are both advertised by the same bit in beacon and probe responses, they cannot be differentiated by clients. Therefore, they cannot both be used by multiple WLANs with the same SSID.
- WLAN WEP is not supported in 1810w Access Point.

- CKIP
- WPA/WPA2

Note

- Although WPA and WPA2 cannot be used by multiple WLANs with the same SSID, you can configure two WLANs with the same SSID with WPA/TKIP with PSK and Wi-Fi Protected Access (WPA)/Temporal Key Integrity Protocol (TKIP) with 802.1X, or with WPA/TKIP with 802.1X or WPA/AES with 802.1X.
- A WLAN configured with TKIP support will not be enabled on an RM3000AC module.

Related Topics

Configuring Static WEP + 802.1X Layer 2 Security Parameters (CLI), on page 1556
Configuring Layer 2 Parameters (GUI), on page 1560
Configuring Static WEP Layer 2 Security Parameters (CLI), on page 1557
Configuring WPA + WPA2 Layer 2 Security Parameters (CLI), on page 1558
Configuring 802.1X Layer 2 Security Parameters (CLI), on page 1560
Configuring Advanced WLAN Properties (CLI), on page 1534
Information About AAA Override, on page 1556

Information About AAA Override

The AAA Override option of a WLAN enables you to configure the WLAN for identity networking. It enables you to apply VLAN tagging, Quality of Service (QoS), and Access Control Lists (ACLs) to individual clients based on the returned RADIUS attributes from the AAA server.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 1534
Prerequisites for Layer 2 Security, on page 1555

How to Configure WLAN Security

Configuring Static WEP + 802.1X Layer 2 Security Parameters (CLI)

Before you begin

You must have administrator privileges.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**security static-wep-key** {**authentication** {**open** | **sharedkey**} | **encryption** {**104** | **40**} [**ascii** | **hex**] {**0** | **8**}} *wep-key wep-key-index1-4* **Example:** `Switch(config-wlan)# security static-wep-key encryption 40 hex 0 test 2`	Configures static WEP security on a WLAN. The keywords and arguments are as follows: • **authentication**—Configures 802.11 authentication. • **encryption**—Sets the static WEP keys and indices. • **open**—Configures open system authentication. • **sharedkey**—Configures shared key authentication. • **104, 40**—Specifies the WEP key size. • **hex, ascii**—Specifies the input format of the key. • *wep-key-index* , *wep-key-index1-4*—Type of password that follows. A value of 0 indicates that an unencrypted password follows. A value of 8 indicates that an AES encrypted follows.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for Layer 2 Security, on page 1555

Configuring Static WEP Layer 2 Security Parameters (CLI)

Before you begin

You must have administrator privileges.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**security static-wep-key** [**authentication** {**open** | **shared**} | **encryption** {**104** | **40**} {**ascii** | **hex**} [**0** | **8**]] **Example:** `Switch(config-wlan)# security static-wep-key authentication open`	The keywords are as follows: • **static-wep-key**—Configures Static WEP Key authentication. • **authentication**—Specifies the authentication type you can set. The values are open and shared. • **encryption**—Specifies the encryption type that you can set. The valid values are 104 and 40. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters. • **ascii**—Specifies the key format as ASCII. • **hex**—Specifies the key format as HEX.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for Layer 2 Security, on page 1555

Configuring WPA + WPA2 Layer 2 Security Parameters (CLI)

Note The default security policy is WPA2.

Before you begin

You must have administrator privileges.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**security wpa** **Example:** `Switch(config-wlan)# security wpa`	Enables WPA.
Step 4	**security wpa wpa1** **Example:** `Switch(config-wlan)# security wpa wpa1`	Enables WPA1.
Step 5	**security wpa wpa1 ciphers** [**aes** | **tkip**] **Example:** `Switch(config-wlan)# security wpa wpa1 ciphers aes`	Specifies the WPA1 cipher. Choose one of the following encryption types: • **aes**—Specifies WPA/AES support. • **tkip**—Specifies WPA/TKIP support.
Step 6	**security wpa wpa2** **Example:** `Switch(config-wlan)# security wpa`	Enables WPA2.
Step 7	**security wpa wpa2 ciphers** [**aes** | **tkip**] **Example:** `Switch(config-wlan)# security wpa wpa2 ciphers tkip`	Configure WPA2 cipher. Choose one of the following encryption types: • **aes**—Specifies WPA/AES support. • **tkip**—Specifies WPA/TKIP support.
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for Layer 2 Security, on page 1555

Configuring 802.1X Layer 2 Security Parameters (CLI)

Before you begin

You must have administrator privileges.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**security dot1x** **Example:** `Switch(config-wlan)# security dot1x`	Specifies 802.1X security.
Step 4	**security** [**authentication-list** *auth-list-name* | **encryption** {**0** | **104** | **40**} **Example:** `Switch(config-wlan)# security encryption 104`	The keywords and arguments are as follows: • **authentication-list**—Specifies the authentication list for IEEE 802.1X. • **encryption**—Specifies the length of the CKIP encryption key. The valid values are 0, 40, and 104. Zero (0) signifies no encryption. This is the default. **Note** All keys in a WLAN must be of the same size.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for Layer 2 Security, on page 1555

Configuring Layer 2 Parameters (GUI)

Before you begin

- You must have administrator privileges.

Procedure

Step 1 Click **Configuration** > **WLAN** > .

The **WLANs** page appears.

Step 2 Click the WLANs profile of the WLAN you want to configure.

The **WLANs** > **Edit** > page appears.

Step 3 Click the **Security** > **Layer 2** > tab.

Note WLAN WEP is not supported in 1810w Access Point.

Parameter	Description
Layer2 Security	Layer 2 security for the selected WLAN. Values are the following: • None—No Layer 2 security selected. • WPA+WPA2—Wi-Fi Protected Access. • 802.1X—WEP 802.1X data encryption type. For information on these settings, see the Layer 2 802.1X Parameters topic. • Static WEP—Static WEP encryption parameters. • Static WEP + 802.1x—Both Static WEP and 802.1X parameters.
MAC Filtering	MAC address filtering. You can locally configure clients by their MAC addresses in the **MAC Filters** > **New page** . You can add a maximum of 12000 local net users. Otherwise, configure the clients on a RADIUS server. **Note** MAC Filtering is also known as MAC Authentication By Pass (MAB).
Fast Transition	Check box to enable or disable a fast transition between access points.
Over the DS	Check box to enable or disable a fast transition over a distributed system.
Reassociation Timeout	Time in seconds after which a fast transition reassociation times out.

To configure the **WPA + WPA2** parameters, provide the following details:

Parameter	Description
WPA Policy	Check box to enable or disable WPA policy.
WPA Encryption	WPA2 encryption type: TKIP or AES. Available only if the WPA policy is enabled.
WPA2 Policy.	Check box to enable or disable WPA2 policy.
WPA2 Encryption	WPA2 encryption type: TKIP or AES. Available only if the WPA2 policy is enabled.

Parameter	Description
Authentication Key Management	The rekeying mechanism parameter.. Values are the following: • 802.1X • CCKM • PSK • 802.1x + CCKM
PSK Format	Enabled when you select the PSK value for Authentication Key Management. Choose ASCII or the HEX format and enter the preshared key.

To configure **802.1x** parameters, provide the following details:

Parameter	Description
802.11 data encryption	WEP 802.11 data encryption type.
Type	Security type.
Key size	Key size. Values are the following: • None • 40 bits • 104 bits The third-party AP WLAN (17) can only be configured with 802.1X encryption. Drop-down configurable 802.1X parameters are not available for this WLAN.

To specify **Static WEP**, configure the following parameters:

Parameter	Description
802.11 Data Encryption	Static WEP encryption type.
Current Key	Displays the current selected key details.
Type	Security type.
Key size	Key size. Values are the following: • Not set • 40 bits • 104 bits

Parameter	Description
Key Index	Key index from 1 to 4. One unique WEP key index can be applied to each WLAN. Because there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer 2 encryption. Because there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer 2 encryption.
Encryption Key	Encryption key.
Key Format	Encryption key format in ASCII or HEX.
Allow Shared Key Authentication	Key authentication that you can enable or disable.

To configure Static WEP + 802.1X Parameters

Parameter	Description
Static WEP Parameters	
802.11 Data Encryption	Static WEP encryption type.
Current Key	Displays the current selected key details.
Type	Security type.
Key size	Key size. Values are the following: • Not set • 40 bits • 104 bits
Key Index	Key index from 1 to 4. The key index is unique per WLAN. You can only have one "key 1" on a given WLAN. You can define up to 4 keys per WLAN, and the switch will announce the key index, to allow clients configured the same way to know what key to use. This is per WLAN. You can configure all your WLANs (up to 512) as WEP if you want, each with up to 4 keys.
Encryption Key	Encryption key.
Key Format	Encryption key format in ASCII or HEX.
Allow Shared Key Authentication	Key authentication that you can enable or disable.
802.1x Parameters	
802.11 Data Encryption	Static WEP encryption type.

Parameter	Description
Type	Security type.
Key size	Key size. Values are the following: • Not set • 40 bits • 104 bits

Step 4 Click **Apply**.

Related Topics

Prerequisites for Layer 2 Security, on page 1555

Additional References

Related Documents

Related Topic	Document Title
WLAN command reference	*WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
Security configuration guide	*Security Configuration Guide (Catalyst 3850 Switches)Security Configuration Guide (Cisco WLC 5700 Series)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

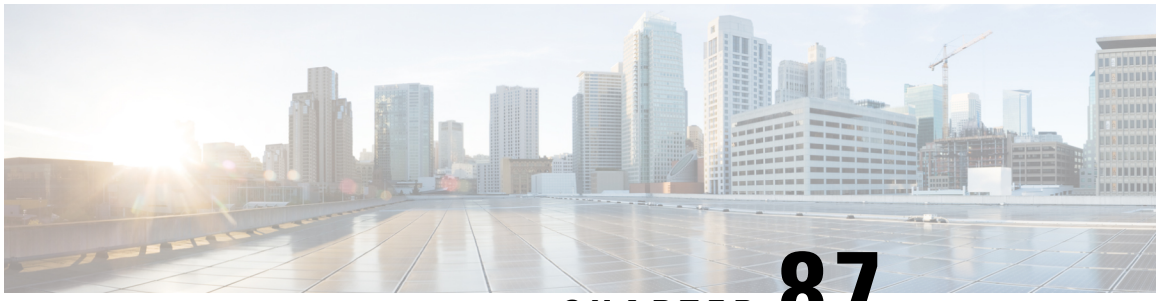
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information about WLAN Layer 2 Security

This table lists the features in this module and provides links to specific configuration information.

Feature Name	Release	Feature Information
WLAN Security functionality	Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 87

Setting Client Count Per WLAN

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Setting Client Count for WLANs

- When a WLAN has reached the limit on the maximum number of clients connected to it or an AP radio and a new client tries to join the WLAN, the client cannot connect to the WLAN until an existing client gets disconnected.
- Roaming clients are considered as new clients. The new client can connect to a WLAN, which has reached the maximum limit on the number of connected clients, only when an existing client gets disconnected.

Note For more information about the number of clients that are supported, see the product data sheet of your switch.

Related Topics

Configuring Client Count per WLAN (CLI), on page 1568

Configuring Client Count Per AP Per WLAN (CLI), on page 1569
Configuring Client Count per AP Radio per WLAN (CLI), on page 1569
Information About Setting the Client Count per WLAN, on page 1568

Information About Setting the Client Count per WLAN

You can set a limit to the number of clients that can connect to a WLAN, which is useful in scenarios where you have a limited number of clients that can connect to a switch. For example, consider a scenario where the switch can serve up to 256 clients on a WLAN and these clients can be shared between enterprise users (employees) and guest users. You can set a limit on the number of guest clients that can access a given WLAN. The number of clients that you can configure for each WLAN depends on the platform that you are using.

Related Topics

Configuring Client Count per WLAN (CLI), on page 1568
Configuring Client Count Per AP Per WLAN (CLI), on page 1569
Configuring Client Count per AP Radio per WLAN (CLI), on page 1569
Restrictions for Setting Client Count for WLANs, on page 1567
Monitoring Client Connections (CLI), on page 1570

How to Configure Client Count Per WLAN

Configuring Client Count per WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**client association limit** *limit* **Example:** `Switch(config-wlan)# client association limit 2000`	Configures the maximum number of client associations per WLAN. The range is 0 to 200012000. A default value is 0 (no limit).
Step 4	**end** **Example:** `Switch(wlan-config)# end`	Returns to priviledged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Related Topics

Information About Setting the Client Count per WLAN, on page 1568
Restrictions for Setting Client Count for WLANs, on page 1567
Monitoring Client Connections (CLI), on page 1570

Configuring Client Count Per AP Per WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**client association limit ap** *ap-limit* **Example:** `Switch(config-wlan)# client association limit ap 250`	Configures the maximum number of clients per AP per WLAN. The range is 1 - 400.
Step 4	**end** **Example:** `Switch(wlan-config)# end`	Returns to priviledged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Related Topics

Information About Setting the Client Count per WLAN, on page 1568
Restrictions for Setting Client Count for WLANs, on page 1567
Monitoring Client Connections (CLI), on page 1570

Configuring Client Count per AP Radio per WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.

	Command or Action	Purpose
Step 3	**client association limit radio** *max-client-connections* **Example:** `Switch(config-wlan)# client association limit radio 180`	Configures the maximum number of client connections per AP radio per WLAN. The range is 0 - 200 for the a, b, and g radios.
Step 4	**end** **Example:** `Switch(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Related Topics

Information About Setting the Client Count per WLAN, on page 1568
Restrictions for Setting Client Count for WLANs, on page 1567
Monitoring Client Connections (CLI), on page 1570

Monitoring Client Connections (CLI)

The following commands can be used to monitor client connections on the switch:

Command	Description

show wlan name *wlan-name*	Displays the WLAN properties. Here is an example:
	`. . . .`
	`Max Associated Clients per WLAN :0`
	`Max Associated Clients per AP per WLAN :0`
	`Max Associated Clients per AP Radio per WLAN :0`
	`. . .`
	`. . .`

show wlan id *wlan-id*	Displays the WLAN properties. here is an example:
	`. . . .`
	`Max Associated Clients per WLAN :0`
	`Max Associated Clients per AP per WLAN :0`
	`Max Associated Clients per AP Radio per WLAN :0`
	`. . .`
	`. . .`

Related Topics

Configuring Client Count per WLAN (CLI), on page 1568
Configuring Client Count Per AP Per WLAN (CLI), on page 1569
Configuring Client Count per AP Radio per WLAN (CLI), on page 1569
Information About Setting the Client Count per WLAN, on page 1568

Additional References for Client Connections

Related Documents

Related Topic	Document Title
WLAN Command References	*WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

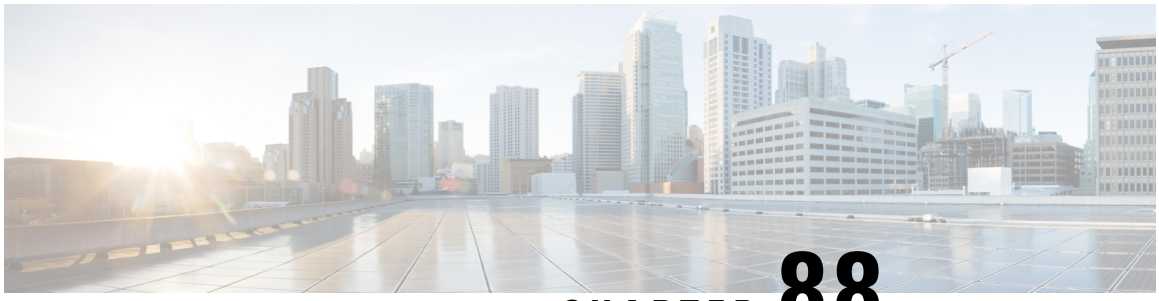
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information about Client Connections Per WLAN

This table lists the features in this module and provides links to specific configuration information:

Feature Name	Release	Feature Information
Client Connections Per WLAN, Per AP, and per AP Radio	Cisco IOS XE 3.3SE	This feature was introduced.



CHAPTER 88

Configuring 802.11w

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for 802.11w

- To configure 802.11w feature for optional and mandatory, you must have WPA and AKM configured.

Note The RNS (Robust Secure Network) IE must be enabled with an AES Cipher.

- To configure 802.11w as mandatory, you must enable PMF AKM in addition to WPA AKM.

Related Topics

Configuring 802.11w (CLI), on page 1575
Disabling 802.11w (CLI), on page 1576

Information About 802.11w, on page 1574

Restrictions for 802.11w

- When 802.11w is set to optional and the keys are set, the AKM suite still shows 802.11w as disabled; this is a Wi-Fi limitation.
- 802.11w cannot be applied on an open WLAN, WEP-encrypted WLAN, or a TKIP-encrypted WLAN.
- The WLAN on which 802.11w is configured must have either WPA2-PSK or WPA2-802.1x security configured.

Related Topics

Configuring 802.11w (CLI), on page 1575
Disabling 802.11w (CLI), on page 1576
Information About 802.11w, on page 1574

Information About 802.11w

Wi-Fi is a broadcast medium that enables any device to eavesdrop and participate either as a legitimate or rogue device. Control and management frames such as authentication/deauthentication, association/disassociation, beacons, and probes are used by wireless clients to select an AP and to initiate a session for network services.

Unlike data traffic which can be encrypted to provide a level of confidentiality, these frames must be heard and understood by all clients and therefore must be transmitted as open or unencrypted. While these frames cannot be encrypted, they must be protected from forgery to protect the wireless medium from attacks. For example, an attacker could spoof management frames from an AP to tear down a session between a client and AP.

The 802.11w protocol applies only to a set of robust management frames that are protected by the Management Frame Protection (PMF) service. These include Disassociation, Deauthentication, and Robust Action frames.

Management frames that are considered as robust action and therefore protected are the following:

- Spectrum Management
- QoS
- Block Ack
- SA Query
- Vendor-specific Protected

When 802.11w is implemented in the wireless medium, the following occur:

- Client protection is added by the AP adding cryptographic protection (by including the MIC information element) to deauthentication and disassociation frames preventing them from being spoofed in a DOS attack.

- Infrastructure protection is added by adding a Security Association (SA) teardown protection mechanism consisting of an Association Comeback Time and an SA-Query procedure preventing spoofed association request from disconnecting an already connected client.

Related Topics

Configuring 802.11w (CLI), on page 1575
Disabling 802.11w (CLI), on page 1576
Prerequisites for 802.11w, on page 1573
Restrictions for 802.11w, on page 1574
Monitoring 802.11w (CLI), on page 1577

How to Configure 802.11w

Configuring 802.11w (CLI)

Before you begin

WPA and AKM must be configured.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**shutdown** **Example:** `Switch shutdown`	Shutdown the WLAN before configuring the PMF.
Step 4	**security pmf** {**association-check** *association-comeback-time-in-seconds* | **mandatory** | **optional** | **saquery** *saquery-time-in-milliseconds*} **Example:** `Switch(config-wlan)# security pmf saquery-retry-time 200`	Configures the PMF parameters with the following options: • **association-comeback**—Configures the 802.11w association comeback time. The range is from 1 to 20 seconds. • **mandatory**—Requires clients to negotiate 802.11w PMF protection on a WLAN. • **optional**—Enables 802.11w PMF protection on a WLAN.

	Command or Action	Purpose
		• **saquery**—Time interval identified in milliseconds before which the SA query response is expected. If the switch does not get a response, another SQ query is tried. The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds.
Step 5	**no shutdown** **Example:** `Switch no shutdown`	Restart the WLAN for the changes to take effect.
Step 6	**end** **Example:** `Switch(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Related Topics

Information About 802.11w, on page 1574
Prerequisites for 802.11w, on page 1573
Restrictions for 802.11w, on page 1574
Monitoring 802.11w (CLI), on page 1577

Disabling 802.11w (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**shutdown** **Example:** `Switch shutdown`	Shutdown the WLAN before configuring the PMF.
Step 4	**no security pmf [association-comeback** *association-check-comback-interval-seconds* |	Disables PMF on the WLAN. The following attributes are available:

	Command or Action	Purpose
	mandatory | **optional** | **saquery** *saquery-time-interval-milliseconds*] **Example:** `Switch(config-wlan)# no security pmf`	• **association-comeback**—Disables the 802.11w association comeback time. • **mandatory**—Disables clients to negotiate 802.11w PMF protection on a WLAN. • **optional**—Disables 802.11w PMF protection on a WLAN. • **saquery**—Time interval identified in the association response to an already associated client before the association can be tried again. This time interval checks if the client is a real client and not a rogue client during the association comeback time. If the client does not respond within this time, the client association is deleted from the switch The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds.
Step 5	**no shutdown** **Example:** `Switch no shutdown`	Restart the WLAN for the changes to take effect.
Step 6	**end** **Example:** `Switch(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Related Topics

Information About 802.11w, on page 1574
Prerequisites for 802.11w, on page 1573
Restrictions for 802.11w, on page 1574
Monitoring 802.11w (CLI), on page 1577

Monitoring 802.11w (CLI)

The following command can be used to monitor 802.11w:

Command	Description
show wlan name *wlan-profile-name*	Displays the WLAN parameters on the WLAN. The PMF parameters are displayed. Here is an example: . . . . Auth Key Management 802.1x : Disabled PSK : Enabled CCKM : Disabled FT dot1x : Disabled FT PSK : Disabled PMF dot1x : Disabled PMF PSK : Enabled FT Support : Disabled FT Reassociation Timeout : 20 FT Over-The-DS mode : Disabled PMF Support : Required PMF Association Comeback Timeout : 9 PMF SA Query Time : 200 . . . .

Related Topics

Configuring 802.11w (CLI), on page 1575
Disabling 802.11w (CLI), on page 1576
Information About 802.11w, on page 1574

Additional References for 802.11w

Related Documents

Related Topic	Document Title
WLAN Command Reference	*WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
WLAN Security	*Configuring WLAN Security* chapter in this book.

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
802.11w	IEEE 802.11w Protected Management Frames

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

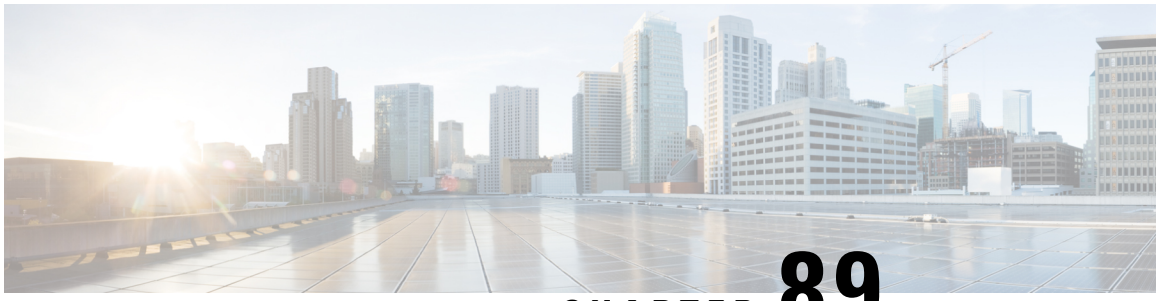
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for 802.11w

This table lists the features in this module and provides links to specific configuration information:

Feature Name	Release	Feature Information
802.11w	Cisco IOS XE 3.3SE	This feature was introduced.



CHAPTER 89

Configuring Wi-Fi Direct Client Policy

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for the Wi-Fi Direct Client Policy

- Wi-Fi Direct Client Policy is applicable to WLANs that have APs in local mode only.
- Cisco APs in FlexConnect mode (even in central authentication and central switching) is not supported.
- We do not recommend enabling this feature in a mixed AP mode deployment (some APs in FlexConnect mode and some APs in local mode). Such types of deployment is not supported or tested in FlexConnect mode.
- If WLAN applied client policy is invalid, the client is excluded with the exclusion reason being 'Client QoS Policy failure'.

Information About the Wi-Fi Direct Client Policy

Devices that are Wi-Fi Direct capable can connect directly to each other quickly and conveniently to do tasks such as printing, synchronization, and sharing of data. Wi-Fi Direct devices may associate with multiple peer-to-peer (P2P) devices and with infrastructure wireless LANs (WLANs) concurrently. You can use the switch to configure the Wi-Fi Direct Client Policy, on a per WLAN basis, where you can allow or disallow association of Wi-Fi devices with infrastructure WLANs, or disable Wi-Fi Direct Client Policy altogether for WLANs.

Related Topics

Configuring the Wi-Fi Direct Client Policy (CLI), on page 1582
Disabling Wi-Fi Direct Client Policy (CLI), on page 1583
Monitoring Wi-Fi Direct Client Policy (CLI), on page 1584

How to Configure Wi-Fi Direct Client Policy

Configuring the Wi-Fi Direct Client Policy (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.

Step 3	**wifidirect policy** {**permit** | **deny** }
	Example:
	`Switch(config-wlan)# wifidirect policy permit`
		Configures the Wi-Fi Direct client policy on the WLAN using one of the following:
		• **permit**—Enables Wi-Fi Direct clients to associate with the WLAN.
		• **deny**—When the Wi-Fi Direct policy is configured as "deny," the switch permits or denies Wi-Fi Direct devices based on the device capabilities. A Wi-Fi Direct device reports these capabilities in its association request to the switch and these are based on the Wi-Fi capabilities of the device. These include:
		  • Concurrent operation
		  • Cross connection

	Command or Action	Purpose
		Note The command **no wifidirect policy** ignores the client's Wi-Fi direct status. Additionally, the access point also does not advertise any beacons and probes. Effectively, the **no** form of the command disables the Wi-Fi direct feature on the WLAN. If the Wi-Fi device supports either concurrent operations or cross connections or both, the client association is denied. The client can associate if the device does not support concurrent operations and cross connections.
Step 4	**end** **Example:** `Switch(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Related Topics

Information About the Wi-Fi Direct Client Policy, on page 1582
Monitoring Wi-Fi Direct Client Policy (CLI), on page 1584

Disabling Wi-Fi Direct Client Policy (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**no wifidirect policy** **Example:** `Switch(config)# no wifidirect policy`	Ignores the Wi-Fi Direct status of clients thereby allowing Wi-Fi Direct clients to associate.

	Command or Action	Purpose
Step 4	**end** **Example:** `Switch(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Related Topics

Information About the Wi-Fi Direct Client Policy, on page 1582
Monitoring Wi-Fi Direct Client Policy (CLI), on page 1584

Monitoring Wi-Fi Direct Client Policy (CLI)

The following commands can be used to monitor Wi-Fi Direct Client Policy:

Command	Description
show wireless client wifidirect stats	Displays the total number of clients associated and the number of association requests rejected if the Wi-Fi Direct Client Policy is enabled.
show wlan summary	Displays status of the Wi-Fi Direct on the WLAN.
show wireless cli mac-address *mac-address*	Displays the detail information of a client.

Related Topics

Configuring the Wi-Fi Direct Client Policy (CLI), on page 1582
Disabling Wi-Fi Direct Client Policy (CLI), on page 1583
Information About the Wi-Fi Direct Client Policy, on page 1582

Additional References for Wi-Fi Direct Client Policy

Related Documents

Related Topic	Document Title
WLAN Command reference	*WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

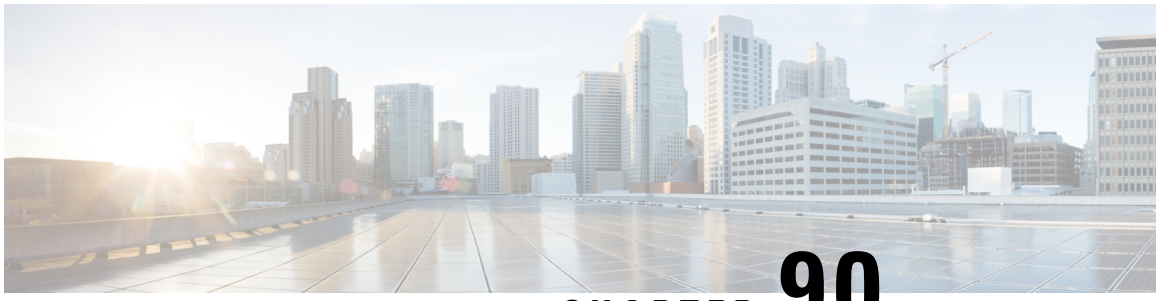
MIB	MIBs Link
All Supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information about Wi-Fi Direct Client Policy

Feature Name	Release	Feature Information
Wi-Fi Direct Feature	Cisco IOS XE 3.3SE	This feature was introduced.



CHAPTER 90

Configuring 802.11r BSS Fast Transition

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for 802.11r Fast Transition

- In 8.1 and earlier releases, this feature is not supported on access points in FlexConnect mode. In Release 8.2, this restriction is removed.
- For access points in FlexConnect mode:
  - 802.11r Fast Transition is supported in central and locally switched WLANs.
  - This feature is not supported for the WLANs enabled for local authentication.
  - 802.11r client association is not supported on access points in standalone mode.
  - 802.11r fast roaming is not supported on access points in standalone mode.
  - 802.11r fast roaming between local authentication and central authentication WLAN is not supported.
  - 802.11r fast roaming works only if the APs are in the same FlexConnect group.

- EAP LEAP method is not supported.
- TSpec is not supported for 802.11r fast roaming. Therefore, RIC IE handling is not supported.
- If WAN link latency exists, fast roaming is also delayed. Voice or data maximum latency should be verified. The Cisco WLC handles 802.11r Fast Transition authentication request during roaming for both Over-the-Air and Over-the-DS methods.
- This feature is supported on open and WPA2 configured WLANs.
- Legacy clients cannot associate with a WLAN that has 802.11r enabled if the driver of the supplicant that is responsible for parsing the Robust Security Network Information Exchange (RSN IE) is old and not aware of the additional AKM suites in the IE. Due to this limitation, clients cannot send association requests to WLANs. These clients, however, can still associate with non-802.11r WLANs. Clients that are 802.11r capable can associate as 802.11i clients on WLANs that have both 802.11i and 802.11r Authentication Key Management Suites enabled.

  The workaround is to enable or upgrade the driver of the legacy clients to work with the new 802.11r AKMs, after which the legacy clients can successfully associate with 802.11r enabled WLANs.

  Another workaround is to have two SSIDs with the same name but with different security settings (FT and non-FT).
- Fast Transition resource request protocol is not supported because clients do not support this protocol. Also, the resource request protocol is an optional protocol.
- To avoid any Denial of Service (DoS) attack, each Cisco WLC allows a maximum of three Fast Transition handshakes with different APs.
- Non-802.11r capable devices will not be able to associate with FT-enabled WLAN.
- 802.11r FT + PMF is not recommended.
- 802.11r FT Over-the-Air roaming is recommended for FlexConnect deployments.
- In a default FlexGroup scenario, fast roaming is not supported.

Related Topics

Configuring 802.11r Fast Transition in an Open WLAN (CLI), on page 1590
Disabling 802.11r Fast Transition (CLI), on page 1595
Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI), on page 1592
Configuring 802.11r Fast Transition on a PSK Security Enabled WLAN (CLI), on page 1593
Configuring 802.11 Fast Transition (GUI), on page 1594
Information About 802.11r Fast Transition, on page 1588

Information About 802.11r Fast Transition

802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP, which is called Fast Transition (FT). The initial handshake allows the client and APs to do the Pairwise Transient Key (PTK) calculation in advance. These PTK keys are applied to the client and AP after the client does the reassociation request or response exchange with new target AP.

802.11r provides two methods of roaming:

- Over-the-Air
- Over-the-DS (Distribution System)

The FT key hierarchy is designed to allow clients to make fast BSS transitions between APs without requiring reauthentication at every AP. WLAN configuration contains a new Authenticated Key Management (AKM) type called FT (Fast Transition).

From Release 3E, you can create an 802.11r WLAN that is also an WPAv2 WLAN. In earlier releases, you had to create separate WLANs for 802.11r and for normal security. Non-802.11r clients can now join 802.11r-enabled WLANs as the 802.11r WLANs can accept non-802.11r associations. If clients do not support mixed mode or 802.11r join, they can join non-802.11r WLANS. When you configure FT PSK and later define PSK, clients that can join only PSK can now join the WLAN in mixed mode.

How a Client Roams

For a client to move from its current AP to a target AP using the FT protocols, the message exchanges are performed using one of the following two methods:

- Over-the-Air—The client communicates directly with the target AP using IEEE 802.11 authentication with the FT authentication algorithm.
- Over-the-DS—The client communicates with the target AP through the current AP. The communication between the client and the target AP is carried in FT action frames between the client and the current AP and is then sent through the switch.

Figure 75: Message Exchanges when Over the Air client roaming is configured

This figure shows the sequence of message exchanges that occur when Over the Air client roaming is configured.

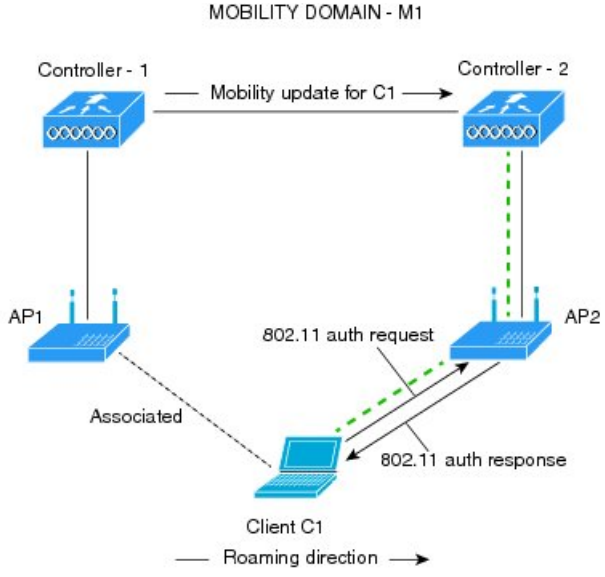
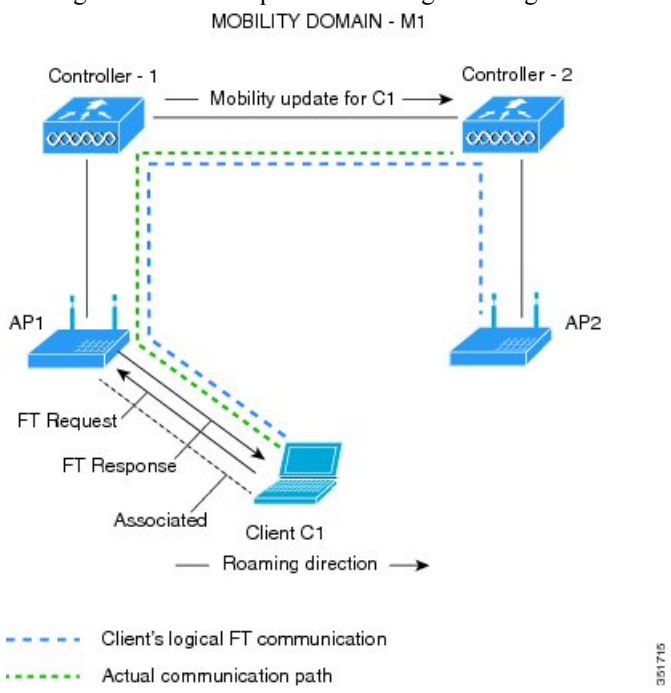


Figure 76: Message Exchanges when Over the DS client roaming is configured

This figure shows the sequence of message exchanges that occur when Over the DS client roaming is configured.



Related Topics

Configuring 802.11r Fast Transition in an Open WLAN (CLI), on page 1590
Disabling 802.11r Fast Transition (CLI), on page 1595
Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI), on page 1592
Configuring 802.11r Fast Transition on a PSK Security Enabled WLAN (CLI), on page 1593
Configuring 802.11 Fast Transition (GUI), on page 1594
Monitoring 802.11r Fast Transition (CLI), on page 1595
Restrictions for 802.11r Fast Transition, on page 1587

How to Configure 802.11r Fast Transition

Configuring 802.11r Fast Transition in an Open WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**client vlan** *vlan-id* **Example:** `Switch(config-wlan)# client vlan 0120`	Associate the client VLAN to the WLAN.
Step 4	**no security wpa** **Example:** `Switch(config-wlan)# no security wpa`	Disable WPA secuirty.
Step 5	**no security wpa akm dot1x** **Example:** `Switch(config-wlan)# no security wpa akm dot1x`	Disable security AKM for dot1x.
Step 6	**no security wpa wpa2** **Example:** `Switch(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 7	**no wpa wpa2 ciphers aes** **Example:** `Switch(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 8	**security ft** **Example:** `Switch(config-wlan)# security ft`	Specifies the 802.11r fast transition parameters.
Step 9	**no shutdown** **Example:** `Switch(config-wlan)# shutdown`	Shutdown the WLAN.
Step 10	**end** **Example:** `Switch(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode

Related Topics

Information About 802.11r Fast Transition, on page 1588
Monitoring 802.11r Fast Transition (CLI), on page 1595
Restrictions for 802.11r Fast Transition, on page 1587

Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**client vlan** *vlan-name* **Example:** `Switch(config-wlan)# client vlan 0120`	Associate the client VLAN to this WLAN.
Step 4	**local-auth** *local-auth-profile-eap* **Example:** `Switch(config-wlan)# local-auth`	Enable the local auth EAP profile.
Step 5	**security dot1x authentication-list default** **Example:** `Switch(config-wlan)# security dot1x authentication-list default`	Enable security authentication list for dot1x security. The configuration is similar for any dot1x security WLAN.
Step 6	**security ft** **Example:** `Switch(config-wlan)# security ft`	Enables 802.11r Fast Transition on this WLAN.
Step 7	**security wpa akm ft dot1x** **Example:** `Switch(config-wlan)# security wpa akm ft dot1x`	Enables 802.1x security on the WLAN.
Step 8	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Enable the WLAN.
Step 9	**end** **Example:** `Switch(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode

Related Topics

Information About 802.11r Fast Transition, on page 1588
Monitoring 802.11r Fast Transition (CLI), on page 1595
Restrictions for 802.11r Fast Transition, on page 1587

Configuring 802.11r Fast Transition on a PSK Security Enabled WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**client vlan** *vlan-name* **Example:** `Switch(config-wlan)# client vlan 0120`	Associates the client VLAN to this WLAN.
Step 4	**no security wpa akm dot1x** **Example:** `Switch(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**security wpa akm ft psk** **Example:** `Switch(config-wlan)# security wpa akm ft psk`	Configures FT PSK support.
Step 6	**security wpa akm psk set-key** {**ascii** {**0** | **8**} | **hex** {**0** | **8**}} **Example:** `Switch(config-wlan)# security wpa akm psk set-key ascii 0 test`	Configures PSK AKM shared key.
Step 7	**security ft** **Example:** `Switch(config-wlan)# security ft`	Configures 802.11r Fast Transition.
Step 8	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Enables the WLAN.

	Command or Action	Purpose
Step 9	**end** **Example:** `Switch(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode

Related Topics

Information About 802.11r Fast Transition, on page 1588
Monitoring 802.11r Fast Transition (CLI), on page 1595
Restrictions for 802.11r Fast Transition, on page 1587

Configuring 802.11 Fast Transition (GUI)

Procedure

Step 1 Click **Configuration** > **Wireless** > **WLANs**

The **WLANs** page is displayed.

Step 2 Locate the WLAN you want to configure by using the search mechanism on the page.

Step 3 Click on the **WLAN Profile** of the WLAN.

The **WLAN > Edit** page is displayed.

Step 4 Click the **Security** and **Layer 2** tab.

Step 5 Enable the **Fast Transition** check box to enable BSS Fast Transition.

Uncheck the **Fast Transition** check box to disable BSS Fast Transition.

Step 6 To enable BSS Fast Transition over the distributed system, enable the **Over the DS** checkbox. This is enabled by default.

Note Disabling over the DS enables over the air fast transition.

Step 7 (Optional) Specify a reassociation timeout value in seconds in the **Reassociation Timeout** text box. The range is 1 to 100 seconds. The default value is 20 seconds.

Step 8 Click **Apply**.

Step 9 To configure the WLAN in 802.11r mixed-mode, choose one of the following options from the **Auth Key Mgmt** drop-down list:

- **FT + 802.1x**
- **FT + PSK**
- **FT + 802.1x +CCKM**

Related Topics

Information About 802.11r Fast Transition, on page 1588
Monitoring 802.11r Fast Transition (CLI), on page 1595

Restrictions for 802.11r Fast Transition, on page 1587

Disabling 802.11r Fast Transition (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**no security ft** [**over-the-ds** | **reassociation-timeout** *timeout-in-seconds*] **Example:** `Switch(config-wlan)# no security ft over-the-ds`	Disables 802.11r Fast Transition on the WLAN. **Note** Disabling 802.11r Fast Transition for over the data source enables over the air fast transition.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Information About 802.11r Fast Transition, on page 1588
Monitoring 802.11r Fast Transition (CLI), on page 1595
Restrictions for 802.11r Fast Transition, on page 1587

Monitoring 802.11r Fast Transition (GUI)

You can view the Authentication Key Management details of a client.

Choose **Monitor > Client**. The Clients page appears. Click the corresponding client to view the client details. In the **General** tab, you can view the Authentication Key Management for the client such as FT, PSK, 802.1x, CCKM, 802.1x + CCKM. If the AKM is for 802.11r mixed mode, then FT-802.1x, FT-802.1x-CCKM, or FT-PSK appears.

Monitoring 802.11r Fast Transition (CLI)

The following command can be used to monitor 802.11r Fast Transition:

Command	Description
show wlan name *wlan-name*	Displays a summary of the configured parameters on the WLAN.

Command	Description
show wireless client mac-address *mac-address*	Displays the summary of the 802.11r authentication key management configuration on a client. . . . . . . Client Capabilities CF Pollable : Not implemented CF Poll Request : Not implemented Short Preamble : Not implemented PBCC : Not implemented Channel Agility : Not implemented Listen Interval : 15 Fast BSS Transition : Implemented Fast BSS Transition Details : Client Statistics: Number of Bytes Received : 9019 Number of Bytes Sent : 3765 Number of Packets Received : 130 Number of Packets Sent : 36 Number of EAP Id Request Msg Timeouts : 0 Number of EAP Request Msg Timeouts : 0 Number of EAP Key Msg Timeouts : 0 Number of Data Retries : 1 Number of RTS Retries : 0 Number of Duplicate Received Packets : 1 Number of Decrypt Failed Packets : 0 Number of Mic Failured Packets : 0 Number of Mic Missing Packets : 0 Number of Policy Errors : 0 Radio Signal Strength Indicator : -48 dBm Signal to Noise Ratio : 40 dB . . . . . . If the AKM for the client is 802.11r mixed mode, the following information appears in the output: . . . . . . Authentication Key Management : FT-PSK . . . . . .

Related Topics

Configuring 802.11r Fast Transition in an Open WLAN (CLI), on page 1590
Disabling 802.11r Fast Transition (CLI), on page 1595
Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI), on page 1592
Configuring 802.11r Fast Transition on a PSK Security Enabled WLAN (CLI), on page 1593
Configuring 802.11 Fast Transition (GUI), on page 1594
Information About 802.11r Fast Transition, on page 1588

Additional References for 802.11r Fast Transition

Related Documents

Related Topic	Document Title
WLAN Command Reference.	*WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
802.11r from IEEE.	IEEE Standard for 802.11r

MIBs

MIB	MIBs Link
All MIBs supported for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

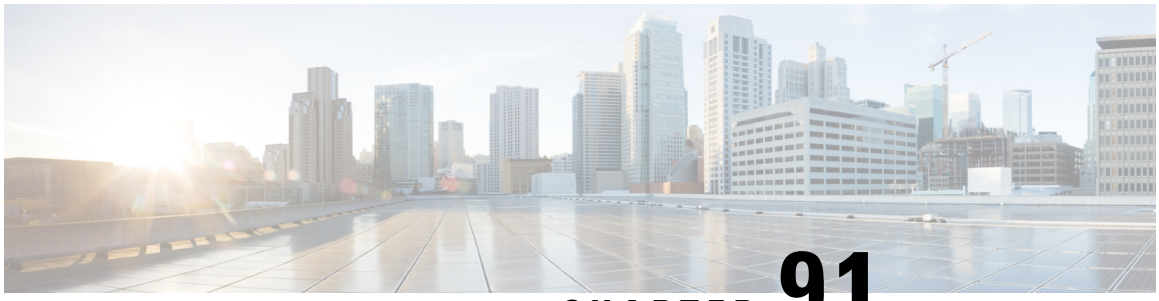
Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for 802.11r Fast Transition

This table lists the features in this module and provides links to specific configuration information:

Feature Name	Release	Feature Information
802.11r Fast Transition	Cisco IOS XE 3.3SE	This feature was introduced.



CHAPTER 91

Configuring Assisted Roaming

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Assisted Roaming

- The assisted roaming feature is supported across multiple switches.
- This feature is supported only on 802.11n capable indoor access points. For a single band configuration, a maximum of 6 neighbors are visible in a neighbor list. For dual band configuration, a maximum of 12 neighbors are visible.
- You can configure assisted roaming only using the switch CLI.

Related Topics

Information About Assisted Roaming, on page 1600

Configuring Assisted Roaming (CLI), on page 1601

Information About Assisted Roaming

The 802.11k standard allows clients to request neighbor reports containing information about known neighbor access points that are candidates for a service set transition. The use of the 802.11k neighbor list can limit the need for active and passive scanning.

The assisted roaming feature is based on an intelligent and client optimized neighbor list.

Unlike the Cisco Client Extension (CCX) neighbor list, the 802.11k neighbor list is generated dynamically on-demand and is not maintained on the switch. The 802.11k neighbor list is based on the location of the clients without requiring the mobility services engine (MSE). Two clients on the same switch but different APs can have different neighbor lists delivered depending on their individual relationship with the surrounding APs.

By default, the neighbor list contains only neighbors in the same band with which the client is associated. However, a switch exists that allows 802.11k to return neighbors in both bands.

Clients send requests for neighbor lists only after associating with the APs that advertize the RRM (Radio Resource Management) capability information element (IE) in the beacon. The neighbor list includes information about BSSID, channel, and operation details of the neighboring radios.

Assembling and Optimizing the Neighbor List

When the switch receives a request for an 802.11k neighbor list, the following occurs:

1. The switch searches the RRM neighbor table for a list of neighbors on the same band as the AP with which the client is currently associated with.
2. The switch checks the neighbors according to the RSSI (Received Signal Strength Indication) between the APs, the current location of the present AP, the floor information of the neighboring AP from Cisco Prime Infrastructure, and roaming history information on the switch to reduce the list of neighbors to six per band. The list is optimized for APs on the same floor.

Assisted Roaming for Non-802.11k Clients

It is also possible to optimize roaming for non-802.11k clients. You can generate a prediction neighbor list for each client without the client requiring to send an 802.11k neighbor list request. When this is enabled on a WLAN, after each successful client association/reassociation, the same neighbor list optimization is applied on the non-802.11k client to generate the neighbor list and store the list in the mobile station software data structure. Clients at different locations have different lists because the client probes are seen with different RSSI values by different neighbors. Because clients usually probe before any association or reassociation, this list is constructed with the most updated probe data and predicts the next AP that the client is likely to roam to.

We discourage clients from roaming to those less desirable neighbors by denying association if the association request to an AP does not match the entries on the stored prediction neighbor list.

Similar to aggressive load balancing, there is a switch to turn on the assisted roaming feature both on a per-WLAN basis and globally. The following options are available:

- Denial count—Maximum number of times a client is refused association.
- Prediction threshold—Minimum number of entries required in the prediction list for the assisted roaming feature to be activated.

Because both load balancing and assisted roaming are designed to influence the AP that a client associates with, it is not possible to enable both the options at the same time on a WLAN.

Related Topics

Configuring Assisted Roaming (CLI), on page 1601
Restrictions for Assisted Roaming, on page 1599
Monitoring Assisted Roaming, on page 1602
Configuration Examples for Assisted Roaming, on page 1603

How to Configure Assisted Roaming

Configuring Assisted Roaming (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wireless assisted-roaming floor-bias** *dBm* **Example:** `Switch(config)# wireless assisted-roaming floor-bias 20`	Configures neighbor floor label bias. The valid range is from 5 to 25 dBm, and the default value is 15 dBm.
Step 3	**wlan** *wlan-id* **Example:** `Switch(config)# wlan wlan1`	Enters the WLAN configuration submode. The *wlan-name* is the profile name of the configured WLAN.
Step 4	**assisted-roaming neighbor-list** **Example:** `Switch(wlan)# assisted-roaming neighbor-list`	Configures an 802.11k neighbor list for a WLAN. By default, assisted roaming is enabled on the neighbor list when you create a WLAN. The **no** form of the command disables assisted roaming neighbor list.
Step 5	**assisted-roaming dual-list** **Example:** `Switch(wlan)# assisted-roaming dual-list`	Configures a dual-band 802.11k dual list for a WLAN. By default, assisted roaming is enabled on the dual list when you create a WLAN. The **no** form of the command disables assisted roaming dual list.

	Command or Action	Purpose
Step 6	**assisted-roaming prediction** **Example:** `Switch(wlan)# assisted-roaming prediction`	Configures assisted roaming prediction list feature for a WLAN. By default, the assisted roaming prediction list is disabled. **Note** A warning message is displayed and load balancing is disabled for the WLAN if load balancing is already enabled for the WLAN.
Step 7	**wireless assisted-roaming prediction-minimum** *count* **Example:** `Switch# wireless assisted-roaming prediction-minimum`	Configures the minimum number of predicted APs required for the prediction list feature to be activated. The default value is 3. **Note** If the number of the AP in the prediction assigned to the client is less than the number that you specify, the assisted roaming feature will not apply on this roam.
Step 8	**wireless assisted-roaming denial-maximum** *count* **Example:** `Switch# wireless assisted-roaming denial-maximum 8`	Configures the maximum number of times a client can be denied association if the association request is sent to an AP does not match any AP on the prediction. The valid range is from 1 to 10, and the default value is 5.
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Information About Assisted Roaming, on page 1600
Restrictions for Assisted Roaming, on page 1599
Monitoring Assisted Roaming, on page 1602
Configuration Examples for Assisted Roaming, on page 1603

Monitoring Assisted Roaming

The following command can be used to monitor assisted roaming configured on a WLAN. .

Command	Description
show wlan id *wlan-id*	Displays the WLAN parameters on the WLAN.

Related Topics

Information About Assisted Roaming, on page 1600
Configuring Assisted Roaming (CLI), on page 1601

Configuration Examples for Assisted Roaming

This example shows how to configure the neighbor floor label bias:

```
Switch# configure terminal
Switch(config)# wireless assisted-roaming floor-bias 10
Switch(config)# end
Switch# show wlan id 23
```

This example shows how to disable neighbor list on a specific WLAN:

```
Switch# configure terminal
Switch(config)# wlan test1
Switch(config (wlan)# no assisted-roaming neighbor-list
Switch(config)(wlan)# end
Switch# show wlan id 23
```

This example shows how to configure the prediction list on a specific WLAN:

```
Switch# configure terminal
Switch(config)# wlan test1
Switch(config)(wlan)# assisted-roaming prediction
Switch(config)(wlan)# end
Switch# show wlan id 23
```

This example shows how to configure the prediction list based on assisted roaming prediction threshold and maximum denial count on a specific WLAN:

```
Switch# configure terminal
Switch(config)# wireless assisted-roaming prediction-minimum 4
Switch(config)# wireless assisted-roaming denial-maximum 4
Switch(config)(wlan)# end
Switch# show wlan id 23
```

Related Topics

Information About Assisted Roaming, on page 1600
Configuring Assisted Roaming (CLI), on page 1601

Additional References for Assisted Roaming

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference (Catalyst 3850 Switches)System Management Command Reference (Cisco WLC 5700 Series)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
802.11k	—

MIBs

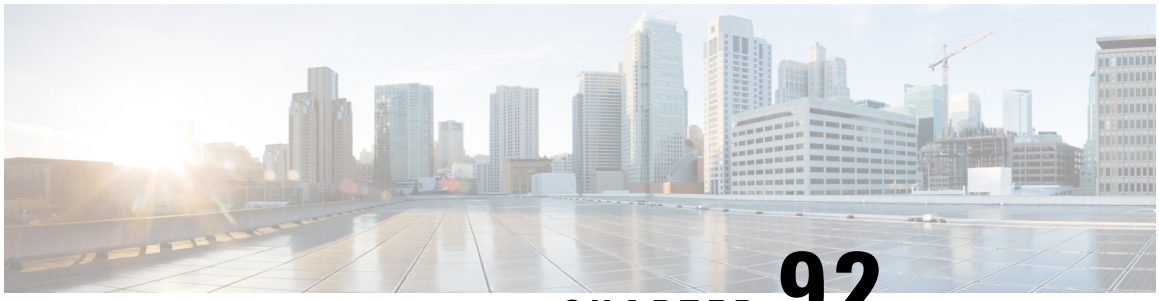
MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Performing Assisted Roaming Configuration

Feature Name	Release	Feature Information
Assisted Roaming	Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 92

Configuring Access Point Groups

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring AP Groups

The following are the prerequisites for creating access point groups on a switch:

- The required access control list (ACL) must be defined on the router that serves the VLAN or subnet.
- Multicast traffic is supported with access point group VLANs. However, if the client roams from one access point to another, the client might stop receiving multicast traffic, unless IGMP snooping is enabled.

Related Topics

Information About Access Point Groups, on page 1606

Restrictions on Configuring Access Point Groups, on page 1606

Restrictions on Configuring Access Point Groups

- Suppose that the interface mapping for a WLAN in the AP group table is the same as the WLAN interface. If the WLAN interface is changed, the interface mapping for the WLAN in the AP group table also changes to the new WLAN interface.

  Suppose that the interface mapping for a WLAN in the AP group table is different from the one defined for the WLAN. If the WLAN interface is changed, then the interface mapping for the WLAN in the AP group table does not change to the new WLAN interface.

- If you clear the configuration on the switch, all of the access point groups disappear except for the default access point group "default-group," which is created automatically.

- The default access point group can have up to 16 WLANs associated with it. The WLAN IDs for the default access point group must be less than or equal to 16. If a WLAN with an ID greater than 16 is created in the default access point group, the WLAN SSID will not be broadcasted. All WLAN IDs in the default access point group must have an ID that is less than or equal to 16. WLANs with IDs greater than 16 can be assigned to custom access point groups.

- We recommend that you configure all Flex+Bridge APs in a mesh tree (in the same sector) in the same AP group and the same FlexConnect group, to inherit the WLAN-VLAN mappings properly.

- Whenever you add a new WLAN to an AP group, radio reset occurs and if any client is in connected state, the client is deauthenticated and is required to reconnect. We recommend that you add or modify the WLAN configuration of an AP group only during maintenance windows to avoid outages.

- The number of AP groups that you can configure cannot be more than the number of ap-count licenses on Cisco WLC. For example, if your Cisco WLC has 5 ap-count licenses, the maximum number of AP groups that you can configure is 5, including the default AP group.

Related Topics

Information About Access Point Groups, on page 1606
Prerequisites for Configuring AP Groups, on page 1605

Information About Access Point Groups

After you create up to 512 WLANs on the switch, you can selectively publish them (using access point groups) to different access points to better manage your wireless network. In a typical deployment, all users on a WLAN are mapped to a single interface on the switch. Therefore, all users that are associated with that WLAN are on the same subnet or VLAN. However, you can choose to distribute the load among several interfaces or to a group of users based on specific criteria such as individual departments (such as Marketing) by creating access point groups. Additionally, these access point groups can be configured in separate VLANs to simplify network administration.

Related Topics

Creating Access Point Groups, on page 1607
Viewing Access Point Group, on page 1608
Assigning an Access Point to an AP Group, on page 1608
Prerequisites for Configuring AP Groups, on page 1605
Restrictions on Configuring Access Point Groups, on page 1606

How to Configure Access Point Groups

Creating Access Point Groups

Before you begin

You must have administrator privileges to perform this operation.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap group** *ap-group-name* **Example:** `Switch(config)# ap group my-ap-group`	Creates an access point group.
Step 3	**wlan** *wlan-name* **Example:** `Switch(config-apgroup)# wlan wlan-name`	Associates the AP group to a WLAN.
Step 4	(Optional) **vlan** *vlan-name* **Example:** `Switch(config-apgroup)# vlan test-vlan`	Assigns the access point group to a VLAN.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Example

This example shows how to create an AP group:

```
Switch# configure terminal
Switch(config-apgroup)# ap group test-ap-group-16
Switch(config-wlan-apgroup)# wlan test-ap-group-16
Switch(config-wlan-apgroup)# vlan VLAN1300
```

Related Topics

Information About Access Point Groups, on page 1606

Assigning an Access Point to an AP Group

Before you begin

You must have administrator privileges to perform this operation.

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap-name* **ap-group-name** *ap-group* **Example:** `Switch# ap name 1240-101 ap-groupname apgroup_16`	Assigns the access point to the access point group. The keywords and arguments are as follows: • **name**—Specifies that the argument following this keyword is the name of an AP that is associated to the switch. • *ap-name*—AP that you want to associate to the AP group. • **ap-group-name**—Specifies that the argument following this keyword is the name of the AP group that is configured on the switch. • *ap-group*—Name of the access point group that is configured on the switch.

Related Topics

Information About Access Point Groups, on page 1606

Viewing Access Point Group

Before you begin

You must have administrator privileges to perform this operation.

Procedure

	Command or Action	Purpose
Step 1	**show ap groups** [**extended**] **Example:** `Switch# show ap groups`	Displays the AP groups configured on the switch. The **extended** keyword displays all AP Groups information defined in the system in detail.

Related Topics

Information About Access Point Groups, on page 1606

Additional References

Related Documents

Related Topic	Document Title
WLAN commands	*WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
Lightweight Access Point configuration	*Lightweight Access Point Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)Lightweight Access Point Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
Lightweight Access Point commands	*Lightweight Access Point Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)Lightweight Access Point Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for Access Point Groups

This table lists the features in this modules and provides links to specific configuration information.

Feature Name	Release	Feature Information
AP Groups	Cisco IOS XE 3.2SE	This feature was introduced.