Cisco Embedded Wireless Controller on Catalyst Access Points Command Reference for Cisco IOS XE Amsterdam 17.2.x

First Published: 2020-03-31

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 switchCiscoEmbedded Wireless Controller, refer to the release notes.

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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.

Using the Command-Line Interface

Information About Using the Command-Line Interface

Note Search options on the GUI and CLI are case sensitive.

Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

You can start a CLI session through a console connection, through Telnet, an SSH, or by using the browser.

When you start a session, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the switch reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the switch reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode .

This table describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode.

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session using Telnet, SSH, or console.	`Device>`	Enter **logout** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.

Mode	Access Method	Prompt	Exit Method	About This Mode
Privileged EXEC	While in user EXEC mode, enter the **enable** command.	`Device#`	Enter **disable** to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	`Device(config)#`	To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**.	Use this mode to configure parameters that apply to the entire switch.
VLAN configuration	While in global configuration mode, enter the **vlan** *vlan-id* command.	`Device(config-vlan)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switch startup configuration file.
Interface configuration	While in global configuration mode, enter the **interface** command (with a specific interface).	`Device(config-if)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the Ethernet ports.
Line configuration	While in global configuration mode, specify a line with the **line vty** or **line console** command.	`Device(config-line)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the terminal line.

Understanding Abbreviated Commands

You need to enter only enough characters for the switch to recognize the command as unique.

This example shows how to enter the **show configuration** privileged EXEC command in an abbreviated form:

```
Device# show conf
```

No and Default Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to reenable a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values.

CLI Error Messages

This table lists some error messages that you might encounter while using the CLI to configure your switch.

Table 2: Common CLI Error Messages

Error Message	Meaning	How to Get Help
`% Ambiguous command: "show con"`	You did not enter enough characters for your switch to recognize the command.	Reenter the command followed by a question mark (?) without any space between the command and the question mark. The possible keywords that you can enter with the command appear.
`% Incomplete command.`	You did not enter all of the keywords or values required by this command.	Reenter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
`% Invalid input detected at '^' marker.`	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all of the commands that are available in this command mode. The possible keywords that you can enter with the command appear.

Configuration Logging

You can log and view changes to the switch configuration. You can use the Configuration Change Logging and Notification feature to track changes on a per-session and per-user basis. The logger tracks each configuration command that is applied, the user who entered the command, the time that the command was entered, and the parser return code for the command. This feature includes a mechanism for asynchronous notification to registered applications whenever the configuration changes. You can choose to have the notifications sent to the syslog.

Note Only CLI or HTTP changes are logged.

Using the Help System

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command.

SUMMARY STEPS

1. **help**
2. *abbreviated-command-entry* **?**
3. *abbreviated-command-entry* <Tab>
4. **?**
5. *command* **?**
6. *command keyword* **?**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**help** **Example:** `Device# help`	Obtains a brief description of the help system in any command mode.

Step 2	*abbreviated-command-entry* **?**
	Example:
	`Device# di?`
	`dir disable disconnect`
		Obtains a list of commands that begin with a particular character string.

Step 3	*abbreviated-command-entry* <Tab>
	Example:
	`Device# sh conf<tab>`
	`Device# show configuration`
		Completes a partial command name.

Step 4	**?** **Example:**	Lists all commands available for a particular command mode.

	Command or Action	Purpose
	`Device> ?`	
Step 5	*command* **?** **Example:** `Device> show ?`	Lists the associated keywords for a command.

Step 6	*command keyword* **?**
	Example:
	`Device(config)# wireless management ?`
	`certificate  Configure certificate details`
	`interface    Select an interface to configure`
	`transfer     Active transfer profiles`
	`trustpoint   Select a trustpoint to configure`
		Lists the associated arguments for a keyword.

Configuration Commands: a to f

aaa accounting identity

To enable authentication, authorization, and accounting (AAA) for IEEE 802.1x, MAC authentication bypass (MAB), and web authentication sessions, use the **aaa accounting identity** command in global configuration mode. To disable IEEE 802.1x accounting, use the **no** form of this command.

aaa accounting identity {*name* | **default**} **start-stop** {**broadcast group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} **. . .**] | **group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} **. . .**]}
no aaa accounting identity {*name* | **default**}

Syntax Description

name	Name of a server group. This is optional when you enter it after the **broadcast group** and **group** keywords.
default	Uses the accounting methods that follow as the default list for accounting services.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested-user process begins regardless of whether or not the start accounting notice was received by the accounting server.
broadcast	Enables accounting records to be sent to multiple AAA servers and send accounting records to the first server in each group. If the first server is unavailable, the uses the list of backup servers to identify the first server.
group	Specifies the server group to be used for accounting services. These are valid server group names: • *name* — Name of a server group. • **radius** — Lists of all RADIUS hosts. • **tacacs+** — Lists of all TACACS+ hosts. The **group** keyword is optional when you enter it after the **broadcast group** and **group** keywords. You can enter more than optional **group** keyword.
radius	(Optional) Enables RADIUS authorization.
tacacs+	(Optional) Enables TACACS+ accounting.

Command Default

AAA accounting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

To enable AAA accounting identity, you need to enable policy mode. To enable policy mode, enter the **authentication display new-style** command in privileged EXEC mode.

This example shows how to configure IEEE 802.1x accounting identity:

```
Device# authentication display new-style

Please note that while you can revert to legacy style
configuration at any time unless you have explicitly
entered new-style configuration, the following caveats
should be carefully read and understood.

(1) If you save the config in this mode, it will be written
    to NVRAM in NEW-style config, and if you subsequently
    reload the router without reverting to legacy config and
    saving that, you will no longer be able to revert.

(2) In this and legacy mode, Webauth is not IPv6-capable. It
    will only become IPv6-capable once you have entered new-
    style config manually, or have reloaded with config saved
    in 'authentication display new' mode.

Device# configure terminal
Device(config)# aaa accounting identity default start-stop group radius
```

aaa accounting update periodic interval-in-minutes

To configure accounting update records intervals, use the **aaa accounting update periodic** command.

aaa accounting update periodic *interval-in-minutes* [**jitter maximum** *jitter-max-value*]

Syntax Description

periodic	Send accounting update records at regular intervals.
<1-71582>	Periodic intervals to send accounting update records(in minutes)
jitter	Set jitter parameters for periodic interval
maximum	Set maximum jitter value for periodic interval (in seconds)
<0-2147483>	Maximum jitter value for periodic interval(in seconds). Default is 300 seconds.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Examples

The following example shows how to configure the interval to five minutes at which the accounting records are updated:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# aaa accounting update periodic 5
```

aaa authentication dot1x

To specify the authentication, authorization, and accounting (AAA) method to use on ports complying with the IEEE 802.1x authentication, use the **aaa authentication dot1x** command in global configuration mode . To disable authentication, use the **no** form of this command.

aaa authentication dot1x {**default**} *method1*
no aaa authentication dot1x {**default**} *method1*

Syntax Description

default	The default method when a user logs in. Use the listed authentication method that follows this argument.
method1	Specifies the server authentication. 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 strings, only the **default** and **group radius** keywords are supported.

Command Default

No authentication is performed.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

The **method** argument identifies the method that the authentication algorithm tries in the specified sequence to validate the password provided by the client. The only method that is IEEE 802.1x-compliant is the **group radius** method, in which the client data is validated against a RADIUS authentication server.

If you specify **group radius**, you must configure the RADIUS server by entering the **radius-server host** global configuration command.

Use the **show running-config** privileged EXEC command to display the configured lists of authentication methods.

This example shows how to enable AAA and how to create an IEEE 802.1x-compliant authentication list. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is not allowed access to the network.

```
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
```

aaa authentication login

To set authentication, authorization, and accounting (AAA) at login, use the **aaa authentication login** command in global configuration mode.

aaa authentication login *authentication-list-name* {**group** }*group-name*

Syntax Description

authentication-list-name	Character string used to name the list of authentication methods activated when a user logs in.
group	Uses a subset of RADIUS servers for authentication as defined by the server group **group-name**.
group-name	Server group name.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None

The following example shows how to set an authentication method list named **local_webauth** to the group type named **local** in local web authentication:

```
Device(config)# aaa authentication login local_webauth local
```

The following example shows how to set an authentication method to RADIUS server group in local web authentication:

```
Device(config)# aaa authentication login webauth_radius group ISE_group
```

aaa authorization

To set the parameters that restrict user access to a network, use the **aaa authorization** command in global configuration mode. To remove the parameters, use the **no** form of this command.

aaa authorization { **auth-proxy** | **cache** | **commands** *level* | **config-commands** | **configuration** | **console** | **credential-download** | **exec** | **multicast** | **network** | **onep** | **policy-if** | **prepaid** | **radius-proxy** | **reverse-access** | **subscriber-service** | **template** } { **default** | *list_name* } [*method1* [*method2* . . .]]

Syntax Description

auth-proxy	Runs authorization for authentication proxy services.
cache	Configures the authentication, authorization, and accounting (AAA) server.
commands	Runs authorization for all commands at the specified privilege level.
level	Specific command level that should be authorized. Valid entries are 0 through 15.
config-commands	Runs authorization to determine whether commands entered in configuration mode are authorized.
configuration	Downloads the configuration from the AAA server.
console	Enables the console authorization for the AAA server.
credential-download	Downloads EAP credential from Local/RADIUS/LDAP.
exec	Enables the console authorization for the AAA server.
multicast	Downloads the multicast configuration from the AAA server.
network	Runs authorization for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Programs (NCPs), and AppleTalk Remote Access (ARA).
onep	Runs authorization for the ONEP service.
reverse-access	Runs authorization for reverse access connections, such as reverse Telnet.
template	Enables template authorization for the AAA server.
default	Uses the listed authorization methods that follow this keyword as the default list of methods for authorization.
list_name	Character string used to name the list of authorization methods.
method1 [*method2...*]	(Optional) An authorization method or multiple authorization methods to be used for authorization. A method may be any one of the keywords listed in the table below.

Command Default

Authorization is disabled for all actions (equivalent to the method keyword **none**).

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

Use the **aaa authorization** command to enable authorization and to create named methods lists, which define authorization methods that can be used when a user accesses the specified function. Method lists for authorization define the ways in which authorization will be performed and the sequence in which these methods will be performed. A method list is a named list that describes the authorization methods (such as RADIUS or TACACS+) that must be used in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, which ensures a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or until all the defined methods are exhausted.

Note The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle--meaning that the security server or the local username database responds by denying the user services--the authorization process stops and no other authorization methods are attempted.

If the **aaa authorization** command for a particular authorization type is issued without a specified named method list, the default method list is automatically applied to all interfaces or lines (where this authorization type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no authorization takes place. The default authorization method list must be used to perform outbound authorization, such as authorizing the download of IP pools from the RADIUS server.

Use the **aaa authorization** command to create a list by entering the values for the *list-name* and the *method* arguments, where *list-name* is any character string used to name this list (excluding all method names) and *method* identifies the list of authorization methods tried in the given sequence.

Note In the table that follows, the **group***group-name*, **group ldap**, **group radius**, and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius server** and **tacacs server** commands to configure the host servers. Use the **aaa group server radius**, **aaa group server ldap**, and **aaa group server tacacs+** commands to create a named group of servers.

This table describes the method keywords.

Table 3: aaa authorization Methods

Keyword	Description
cache *group-name*	Uses a cache server group for authorization.

Keyword	Description
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the **server group** *group-name* command.
group ldap	Uses the list of all Lightweight Directory Access Protocol (LDAP) servers for authentication.
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.
grouptacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
if-authenticated	Allows the user to access the requested function if the user is authenticated. **Note** The **if-authenticated** method is a terminating method. Therefore, if it is listed as a method, any methods listed after it will never be evaluated.
local	Uses the local database for authorization.
none	Indicates that no authorization is performed.

Cisco IOS software supports the following methods for authorization:

- Cache Server Groups—The router consults its cache server groups to authorize specific rights for users.
- If-Authenticated—The user is allowed to access the requested function provided the user has been authenticated successfully.
- Local—The router or access server consults its local database, as defined by the **username** command, to authorize specific rights for users. Only a limited set of functions can be controlled through the local database.
- None—The network access server does not request authorization information; authorization is not performed over this line or interface.
- RADIUS—The network access server requests authorization information from the RADIUS security server group. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.
- TACACS+—The network access server exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value (AV) pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.

Method lists are specific to the type of authorization being requested. AAA supports five different types of authorization:

- Commands—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- EXEC—Applies to the attributes associated with a user EXEC terminal session.
- Network—Applies to network connections. The network connections can include a PPP, SLIP, or ARA connection.

Note You must configure the **aaa authorization config-commands** command to authorize global configuration commands, including EXEC commands prepended by the **do** command.

- Reverse Access—Applies to reverse Telnet sessions.
- Configuration—Applies to the configuration downloaded from the AAA server.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, the method lists must be applied to specific lines or interfaces before any of the defined methods are performed.

The authorization command causes a request packet containing a series of AV pairs to be sent to the RADIUS or TACACS daemon as part of the authorization process. The daemon can do one of the following:

- Accept the request as is.
- Make changes to the request.
- Refuse the request and authorization.

For a list of supported RADIUS attributes, see the module RADIUS Attributes. For a list of supported TACACS+ AV pairs, see the module TACACS+ Attribute-Value Pairs.

Note Five commands are associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included in the privilege level command set.

The following example shows how to define the network authorization method list named mygroup, which specifies that RADIUS authorization will be used on serial lines using PPP. If the RADIUS server fails to respond, local network authorization will be performed.

```
Device(config)#  aaa authorization network mygroup group radius local
```

aaa authorization credential download default

To set an authorization method list to use local credentials, use the **aaa authorization credential download default** command in global configuration mode.

aaa authorization credential download default *group-name*

Syntax Description

group-name	Server group name.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

The following example shows how to set an authorization method list to use local credentials:

```
Device(config)# aaa authorization credential-download default local
```

aaa group server ldap

To configure a AAA server group, use the **aaa group server ldap** command.

aaa group server ldap *group-name*

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure a AAA server group:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# aaa new-model
Device(config)# aaa group server ldap name1
Device(config-ldap-sg)# server server1
Device(config-ldap-sg)# exit
```

aaa group server radius

To group different RADIUS server hosts into distinct lists and distinct methods, use the **aaa group server radius** command in global configuration mode.

aaa group server radius *group-name*

Syntax Description

group-name	Character string used to name the group of servers.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

The authentication, authorization, and accounting (AAA) server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

A group server is a list of server hosts of a particular type. Currently supported server host types are RADIUS server hosts. A group server is used in conjunction with a global server host list. The group server lists the IP addresses of the selected server hosts.

The following example shows how to configure an AAA group server named **ISE_Group** that comprises three member servers:

```
Device(config)# aaa group server radius ISE_Group
```

aaa local authentication default authorization

To configure local authentication method list, use the **aaa local authentication default authorization** command.

aaa local authentication default authorization [*method-list-name* | **default**]

Syntax Description

method-list-name	Name of the method list.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure local authentication method list to the default list:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# aaa local authentication default authorization default
```

aaa new-model

To enable the authentication, authorization, and accounting (AAA) access control model, issue the **aaa new-model** command in global configuration mode. To disable the AAA access control model, use the **no** form of this command.

aaa new-model
no aaa new-model

Syntax Description

This command has no arguments or keywords.

Command Default

AAA is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

This command enables the AAA access control system.

If the **login local** command is configured for a virtual terminal line (VTY), and the **aaa new-model** command is removed, you must reload the to get the default configuration or the **login** command. If the is not reloaded, the defaults to the **login local** command under the VTY.

Note We do not recommend removing the **aaa new-model** command.

The following example shows this restriction:

```
Device(config)# aaa new-model
Device(config)# line vty 0 15
Device(config-line)# login local
Device(config-line)# exit
Device(config)# no aaa new-model
Device(config)# exit
Device# show running-config | b line vty

line vty 0 4
 login local  !<=== Login local instead of "login"
line vty 5 15
 login local
!
```

Examples

The following example initializes AAA:

```
Device(config)# aaa new-model
Device(config)#
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication arap	Enables an AAA authentication method for ARAP using TACACS+.
aaa authentication enable default	Enables AAA authentication to determine if a user can access the privileged command level.
aaa authentication login	Sets AAA authentication at login.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.

aaa server radius dynamic-author

To configure a device as an authentication, authorization, and accounting (AAA) server to facilitate interaction with an external policy server, use the **aaa server radius dynamic-author**command in global configuration mode. To remove this configuration, use the **no** form of this command.

aaa server radius dynamic-author
no aaa server radius dynamic-author

Syntax Description

This command has no arguments or keywords.

Command Default

The device will not function as a server when interacting with external policy servers.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
12.2(5)SXI	This command was integrated into Cisco IOS Release 12.2(5)SXI.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

Dynamic authorization allows an external policy server to dynamically send updates to a device. Once the **aaa server radius dynamic-author** command is configured, dynamic authorization local server configuration mode is entered. Once in this mode, the RADIUS application commands can be configured.

Dynamic Authorization for the Intelligent Services Gateway (ISG)

ISG works with external devices, referred to as policy servers, that store per-subscriber and per-service information. ISG supports two models of interaction between the ISG device and external policy servers: initial authorization and dynamic authorization.

The dynamic authorization model allows an external policy server to dynamically send policies to the ISG. These operations can be initiated in-band by subscribers (through service selection) or through the actions of an administrator, or applications can change policies on the basis of an algorithm (for example, change session quality of service (QoS) at a certain time of day). This model is facilitated by the Change of Authorization (CoA) RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling ISG and the external policy server each to act as a RADIUS client and server.

Examples

The following example configures the ISG to act as a AAA server when interacting with the client at IP address 10.12.12.12:

```
aaa server radius dynamic-author
```

```
client 10.12.12.12 key cisco
message-authenticator ignore
```

Related Commands

Command	Description
auth-type (ISG)	Specifies the server authorization type.
client	Specifies a RADIUS client from which a device will accept CoA and disconnect requests.
default	Sets a RADIUS application command to its default.
domain	Specifies username domain options.
ignore	Overrides a behavior to ignore certain paremeters.
port	Specifies a port on which local RADIUS server listens.
server-key	Specifies the encryption key shared with RADIUS clients.

aaa session-id

To specify whether the same session ID will be used for each authentication, authorization, and accounting (AAA) accounting service type within a call or whether a different session ID will be assigned to each accounting service type, use the **aaa session-id** command in global configuration mode. To restore the default behavior after the **unique** keyword is enabled, use the **no** form of this command.

aaa session-id [{**common** | **unique**}]
no aaa session-id [**unique**]

Syntax Description

common	(Optional) Ensures that all session identification (ID) information that is sent out for a given call will be made identical. The default behavior is **common**.
unique	(Optional) Ensures that only the corresponding service access-requests and accounting-requests will maintain a common session ID. Accounting-requests for each service will have a different session ID.

Command Default

The **common**keyword is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE 16.12.1	This command was integrated in Cisco IOS XE 16.12.1.

Usage Guidelines

The **common**keywordbehaviorallows the first session ID request of the call to be stored in a common database; all proceeding session ID requests will retrieve the value of the first session ID. Because a common session ID is the default behavior, this functionality is written to the system configuration after the **aaa new-model**command is configured.

Note The router configuration will always have either the **aaa session-id common** or the **aaa session-id unique** command enabled; it is not possible to have neither of the two enabled. Thus, the **no aaa session-id unique** command will revert to the default functionality, but the **no aaa session-id common** command will not have any effect because it is the default functionality.

The **unique** keyword behavior assigns a different session ID for each accounting type (Auth-Proxy, Exec, Network, Command, System, Connection, and Resource) during a call. To specify this behavior, the unique keyword must be specified. The session ID may be included in RADIUS access requests by configuring the **radius-server attribute 44 include-in-access-req**command. The session ID in the access-request will be the same as the session ID in the accounting request for the same service; all other services will provide unique session IDs for the same call.

Examples

The following example shows how to configure unique session IDs:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
aaa session-id unique
```

Related Commands

Command	Description
aaa new model	Enables AAA.
radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication).

aaa-override

To enable AAA override on the WLAN, use the **aaa-override** command. To disable AAA override, use the **no** form of this command.

aaa-override
no aaa-override

Syntax Description

This command has no keywords or arguments.

Command Default

AAA is disabled by default.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable AAA on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# aaa-override
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to disable AAA on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# no aaa-override
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

aaa-policy

To map a AAA policy in a WLAN policy profile, use the **aaa-policy** command.

aaa-policy *aaa-policy-name*

Syntax Description

aaa-policy-name	Name of the AAA policy.

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to map a AAA policy in a WLAN policy profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-name
Device(config-wireless-policy)# aaa-policy aaa-policy-name
```

aaa-realm enable

To enable AAA RADUIS selection by realm, use the **aaa-realm enable** command.

aaa-realm enable

Command Default None

Command Modes config-aaa-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to enable AAA RADIUS section by realm:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless aaa policy aaa-profile-name
Device (config-aaa-policy)#  aaa-realm enable
```

absolute-timer

To enable an absolute timeout for subscriber sessions, use the **absolute-timer** command in service template configuration mode. To disable the timer, use the **no** form of this command.

absolute-timer *minutes*
no absolute-timer

Syntax Description

minutes	Maximum session duration, in minutes. Range: 1 to 65535. Default: 0, which disables the timer.

Command Default

Disabled (the absolute timeout is 0).

Command Modes

Service template configuration (config-service-template)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **absolute-timer** command to limit the number of minutes that a subscriber session can remain active. After this timer expires, a session must repeat the process of establishing its connection as if it were a new request.

Examples

The following example shows how to set the absolute timeout to 15 minutes in the service template named SVC_3:

```
service-template SVC_3
 description sample
 access-group ACL_2
 vlan 113
 inactivity-timer 15
 absolute-timer 15
```

Related Commands

Command	Description
event absolute-timeout	Specifies the type of event that triggers actions in a control policy if conditions are met.
inactivity-timer	Enables an inactivity timeout for subscriber sessions.
show service-template	Displays configuration information for service templates.

access-list

To add an access list entry, use the **access-list** command.

access-list {*1-99* *100-199* *1300-1999* *2000-2699*} [*sequence-number*] { **deny** | **permit** } { *hostname-or-ip-addr* [{*wildcard-bits* | **log**}] | **any** [**log**] | **host** *hostname-or-ip-addr* **log**} | {**remark** [*line*] }

Syntax Description

1-99	Configures IP standard access list.
100-199	Configures IP extended access list.
1300-1999	Configures IP standard access list (expanded range).
2000-2699	Configures IP extended access list (expanded range).
sequence-number	Sequence number of the ACL entry. Valid range is 1 to 2147483647.
deny	Configures packets to be rejected.
permit	Configures packets to be forwarded.
hostname-or-ip-addr	Hostname or the IP address to match.
wildcard-bits	Wildcard bits to match the IP address.
log	Configures log matches against this entry.
any	Any source host.
host	A single host address.
remark	Configures ACL entry comment.
line	The ACL entry comment.

Command Default

None

Command Modes

Global Config

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to add an access list entry:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# access-list 1 permit any
```

access-list acl-ace-limit

To set the maximum configurable ace limit for all ACLs, use the **access-list acl-ace-limit** command.

access-list acl-ace-limit *max-ace-limit*

Syntax Description

max-ace-limit	Maximum number of ace limit for all ACLs. Valid range is 1 to 4294967295.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to set the maximum configurable ace limit for all ACLs to 100:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# access-list acl-ace-limit 100
```

accounting-list

To configure RADIUS accounting servers on , use the **accounting-list** command. To disable RADIUS server accounting, use the **no** form of this command.

accounting-list *radius-server-acct*
no accounting-list

Syntax Description

radius-server-acct	Accounting RADIUS server name.

Command Default

RADIUS server accounting is disabled by default.

Command Modes

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to configure RADIUS server accounting on :

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#
Deviceaccounting-list test
Device
```

This example shows how to disable RADIUS server accounting on :

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#
Deviceno accounting-list test
Device
```

acl-policy

To configure an access control list (ACL) policy, use the **acl-policy** command.

acl-policy *acl-policy-name*

Syntax Description

acl-policy-name	Name of the ACL policy.

Command Default

None

Command Modes

config-wireless-flex-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure an ACL policy name:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# acl-policy my-acl-policy
```

address

To specify the IP address of the Rivest, Shamir, and Adelman (RSA) public key of the remote peer that you will manually configure in the keyring, use the **address** command inrsa-pubkey configuration mode. To remove the IP address, use the **no** form of this command.

address *ip-address*
no address *ip-address*

Syntax Description

ip-address	IP address of the remote peer.

Command Default

No default behavior or values

Command Modes

Rsa-pubkey configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
Cisco IOS XE 16.12.1	This command was integrated into Cisco ISO XE 16.12.1

Usage Guidelines

Before you can use this command, you must enter the **rsa-pubkey** command in the crypto keyring mode.

Examples

The following example specifies the RSA public key of an IP Security (IPSec) peer:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

Related Commands

Command	Description
crypto keyring	Defines a crypto keyring to be used during IKE authentication.
key-string	Specifies the RSA public key of a remote peer.
rsa-pubkey	Defines the RSA manual key to be used for encryption or signatures during IKE authentication.

address prefix

To specify an address prefix for address assignment, use the **address prefix** command in interface configuration mode. To remove the address prefix, use the **no** form of this command.

address prefix ipv6-prefix [**lifetime** {**valid-lifetime preferred-lifetime** | **infinite**}]
no address prefix

Syntax Description

ipv6-prefix	IPv6 address prefix.
lifetime {valid-lifetime preferred-lifetime | infinite}]	(Optional) Specifies a time interval (in seconds) that an IPv6 address prefix remains in the valid state. If the **infinite** keyword is specified, the time interval does not expire.

Command Default

No IPv6 address prefix is assigned.

Command Modes

DHCP pool configuration (config-dhcpv6)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

You can use the **address prefix** command to configure one or several address prefixes in an IPv6 DHCP pool configuration. Each time the IPv6 DHCP address pool is used, an address will be allocated from each of the address prefixes associated with the IPv6 DHCP pool.

Examples

The following example shows how to configure a pool called engineering with an IPv6 address prefix:

```
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# address prefix 2001:1000::0/64 lifetime infinite
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCPv6 server configuration information pool and enters DHCPv6 pool configuration mode.

allow at-least min-number at-most max-number

To limit the number of multicast RAs per device per throttle period in an RA throttler policy, use the **allow at-least** *min-number* **at-most** *max-number* command.

allow at-least *min-number* **at-most** {*max-number* | **no-limit**}

Syntax Description

at-least *min-number*	Enter the minimum guaranteed number of multicast RAs per router before throttling can be enforced. Valid range is 0 to 32.
at-most *max-number*	Enter the maximum number of multicast RAs from router by which throttling is enforced. Valid range is 0 to 256.
at-most no-limit	No upper bound at the router level.

Command Default

None

Command Modes

config-nd-ra-throttle

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to limit the number of multicast RAs per device per throttle period in an RA throttler policy:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ipv6 nd ra-throttler policy ra-throttler-policy-name
Device(config-nd-ra-throttle)# allow at-least 5 at-most 10
```

ap

To configure cisco APs, use the **ap** command.

ap *mac-address*

Syntax Description

mac-address	Ethernet MAC address of the AP.

Command Default

None

Command Modes

config

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

none.

Example

The following example shows how to configure a Cisco AP:

```
Device(config)# ap F866.F267.7DFB
```

ap auth-list

To configure the AP authorization list, use the **ap auth-list** command in the global configuration mode. To disable the AP authorization list, use the **no** form of this command.

ap auth-list {**authorize-mac** | **authorize-serialNum** | **method-list** *method-list-name*}

no ap auth-list {**authorize-mac** | **authorize-serialNum** | **method-list** *method-list-name*}

Syntax Description

authorize-mac	Configures the AP authorization policy with MAC.
auhorize-serialNum	Configures the AP authorization policy with the serial number.
method-list	Configures the AP authorization method list.
method-list-name	Indicates the method list name.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Example

The following example shows how to configure the AP authorization policy with serial number:

```
Device(config) #ap auth-list authorize-serialNum
```

ap auth-list ap-policy

To configure authorization policy for all Cisco lightweight access points joined to the switch, use the **ap auth-list ap-policy** command. To disable authorization policy for all Cisco lightweight access points joined to the switch, use the **no** form of this command.

ap auth-list ap-policy {**authorize-ap** | **lsc** | **mic** | **ssc**}
no ap auth-list ap-policy {**authorize-ap** | **lsc** | **mic** | **ssc**}

Syntax Description

authorize-ap	Enables the authorization policy.
lsc	Enables access points with locally significant certificates to connect.
mic	Enables access points with manufacture-installed certificates to connect.
ssc	Enables access points with self signed certificates to connect.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to enable the access point authorization policy:

```
Device(config)# ap auth-list ap-policy authorize-ap
```

This example shows how to enable access points with locally significant certificates to connect:

```
Device(config)# ap auth-list ap-policy lsc
```

This example shows how to enable access points with manufacture-installed certificates to connect:

```
Device(config)# ap auth-list ap-policy mic
```

This example shows how to enable access points with self-signed certificates to connect:

```
Device(config)# ap auth-list ap-policy ssc
```

ap capwap retransmit

To configure Control and Provisioning of Wireless Access Points (CAPWAP) control packet retransmit count and control packet retransmit interval under the AP profile, use the **ap capwap retransmit** command.

ap profile default-ap-profile

ap capwap retransmit {**count** *retransmit-count* | **interval** *retransmit-interval*}

Syntax Description

count *retransmit-count*	Specifies the access point CAPWAP control packet retransmit count. **Note** The count is from 3 to 8 seconds.
interval *retransmit-interval*	Specifies the access point CAPWAP control packet retransmit interval. **Note** The interval is from 2 to 5 seconds.

Command Default

None

Command Modes

AP profile configuration (config-ap-profile)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure the CAPWAP control packet retransmit count for an access point:

```
Device(config)# ap profile default-ap-profile
```

This example shows how to configure the CAPWAP control packet retransmit interval for an access point:

```
Device(config-ap-profile)# capwap retransmit count 3
```

ap capwap timers

To configure advanced timer settings under the AP profile mode, use the **ap capwap timers** command.

ap profile default-ap-profile

ap capwap timers {**discovery-timeout** *seconds* | **fast-heartbeat-timeout local** *seconds* | **heartbeat-timeout** *seconds* | **primary-discovery-timeout** *seconds* | **primed-join-timeout** *seconds*}

Syntax Description

discovery-timeout	Specifies the Cisco lightweight access point discovery timeout. **Note** The Cisco lightweight access point discovery timeout is how long a Cisco switch waits for an unresponsive access point to answer before considering that the access point failed to respond.
seconds	Cisco lightweight access point discovery timeout from 1 to 10 seconds. **Note** The default is 10 seconds.
fast-heartbeat-timeout local	Enables the fast heartbeat timer that reduces the amount of time it takes to detect a switch failure for local or all access points.
seconds	Small heartbeat interval (from 1 to 10 seconds) that reduces the amount of time it takes to detect a switch failure. **Note** The fast heartbeat time-out interval is disabled by default.
heartbeat-timeout	Specifies the Cisco lightweight access point heartbeat timeout. **Note** The Cisco lightweight access point heartbeat timeout controls how often the Cisco lightweight access point sends a heartbeat keep-alive signal to the Cisco switch. This value should be at least three times larger than the fast heartbeat timer.
seconds	Cisco lightweight access point heartbeat timeout value from 1 to 30 seconds. **Note** The default is 30 seconds.
primary-discovery-timeout	Specifies the access point primary discovery request timer. The timer determines the amount of time taken by an access point to discovery the configured primary, secondary, or tertiary switch.
seconds	Access point primary discovery request timer from 30 to 3600 seconds. **Note** The default is 120 seconds.

primed-join-timeout	Specifies the authentication timeout. Determines the time taken by an access point to determine that the primary switch has become unresponsive. The access point makes no further attempts to join the switch until the connection to the switch is restored.
seconds	Authentication response timeout from 120 to 43200 seconds. **Note** The default is 120 seconds.

Command Default

None

Command Modes

AP profile mode (config-ap-profile)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure an access point discovery timeout with the timeout value of 7:

```
Device(config)# ap profile default-ap-profile

Device(config-ap-profile)# ap capwap timers discovery-timeout 7
```

This example shows how to enable the fast heartbeat interval for all access points:

```
Device(config)# ap profile default-ap-profile

Device(config-ap-profile)# ap capwap timers fast-heartbeat-timeout 6
```

This example shows how to configure an access point heartbeat timeout to 20:

```
Device(config)# ap profile default-ap-profile

Device(config-ap-profile)# ap capwap timers heartbeat-timeout 20
```

This example shows how to configure the access point primary discovery request timer to 1200 seconds:

```
Device(config)# ap profile default-ap-profile

Device(config-ap-profile)# ap capwap timers primary-discovery-timeout 1200
```

This example shows how to configure the authentication timeout to 360 seconds:

```
Device(config)# ap profile default-ap-profile

Device(config-ap-profile)# ap capwap timers primed-join-timeout 360
```

ap country

To configure one or more country codes for a switch, use the **ap country** command.

ap country *country-code*

Syntax Description

country-code	Two-letter or three-letter country code or several country codes separated by a comma.

Command Default

US (country code of the United States of America).

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.1	This command has been deprecated. **Note** From Cisco IOS XE Amsterdam 17.3.1 onwards, the command **ap country** is deprecated and renamed as **wireless country** *<1 country code>*, where you can enter country codes for more than 20 countries. Although the existing command **ap country** is still functional, it is recommended that you use the **wireless country** *<1 country code>* command.

Usage Guidelines

The Cisco switch must be installed by a network administrator or qualified IT professional and the installer must select the proper country code. Following installation, access to the unit should be password protected by the installer to maintain compliance with regulatory requirements and to ensure proper unit functionality. See the related product guide for the most recent country codes and regulatory domains.

This example shows how to configure country codes on the switch to IN (India) and FR (France):

```
Device(config)# ap country IN,FR
```

ap dot11

To configure Spectrum Intelligence (SI) on Qualcomm based 2.4 GHz or 5 GHz radios, use the **ap dot11 SI** command.

ap dot11 {**24ghz** | **5ghz** } **SI**

Syntax Description

24ghz	2.4 GHz radio
5ghz	5 GHz radio
SI	Enable Spectrum Intelligence (SI). [no] in the command disasbles SI.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to enable SI on 5GHz radio:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 5ghz SI
```

ap dot11 24ghz cleanair

To enable CleanAir for detecting 2.4-GHz devices, use the **ap dot11 24ghz cleanair** command in global configuration mode. To disable CleanAir for detecting 2.4-GHz devices, use the **no** form of this command.

ap dot11 24ghz cleanair

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

You must enable this CleanAir command before you configure other CleanAir commands.

This example shows how to enable CleanAir for 2.4-GHz devices:

```
Device(config)# ap dot11 24ghz cleanair
```

ap dot11 24ghz dot11g

To enable the Cisco wireless LAN solution 802.11g network, use the **ap dot11 24ghz dot11g** command. To disable the Cisco wireless LAN solution 802.11g network, use the **no** form of this command.

ap dot11 24ghz dot11g
no ap dot11 24ghz dot11g

Syntax Description

This command has no keywords and arguments.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

Before you enter the **ap dot11 24ghz dot11g** command, disable the 802.11 Cisco radio with the **ap dot11 24ghz shutdown** command.

After you configure the support for the 802.11g network, use the **no ap dot11 24ghz shutdown** command to enable the 802.11 2.4 Ghz radio.

This example shows how to enable the 802.11g network:

```
Device(config)# ap dot11 24ghz dot11g
```

ap dot11 24ghz rate

To configure 802.11b operational rates, use the **ap dot11 24ghz rate** command.

ap dot11 24ghz rate {**RATE_11M** | **RATE_12M** | **RATE_18M** | **RATE_1M** | **RATE_24M** | **RATE_2M** | **RATE_36M** | **RATE_48M** | **RATE_54M** | **RATE_5_5M** | **RATE_6M** | **RATE_9M**} {**disable** | **mandatory** | **supported**}

Syntax Description

RATE_11M	Configures the data to be transmitted at the rate of 11 Mbps
RATE_12M	Configures the data to be transmitted at the rate of 12 Mbps
RATE_18M	Configures the data to be transmitted at the rate of 18 Mbps
RATE_1M	Configures the data to be transmitted at the rate of 1 Mbps
RATE_24M	Configures the data to be transmitted at the rate of 24 Mbps
RATE_2M	Configures the data to be transmitted at the rate of 2 Mbps
RATE_36M	Configures the data to be transmitted at the rate of 36 Mbps
RATE_48M	Configures the data to be transmitted at the rate of 48 Mbps
RATE_54M	Configures the data to be transmitted at the rate of 54 Mbps
RATE_5_5M	Configures the data to be transmitted at the rate of 5.5 Mbps
RATE_6M	Configures the data to be transmitted at the rate of 6 Mbps
RATE_9M	Configures the data to be transmitted at the rate of 9 Mbps
disable	Disables the data rate that you specify. Also defines that the clients specify the data rates used for communication.
mandatory	Defines that the clients support this data rate in order to associate with an AP.
supported	Any associated clients support this data rate can communicate with the AP using this rate. However, the clients are not required to use this rate to associate with the AP.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure 802.11b operational rate to 9 Mbps and make it mandatory:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 24ghz rate RATE_9M mandatory
```

ap dot11 rrm channel cleanair-event

To configure CleanAir event-driven Radio Resource Management (RRM) parameters for all 802.11 Cisco lightweight access points, use the **ap dot11 rrm channel cleanair-event** command. When this parameter is configured, CleanAir access points can change their channel when a source of interference degrades the operations, even if the RRM interval has not expired yet.

ap dot11 {**24ghz** | **5ghz**} **rrm channel** {**cleanair-event sensitivity** *value*}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
sensitivity	Sets the sensitivity for CleanAir event-driven RRM.
value	Sensitivity value. You can specify any one of the following three optional sensitivity values: • **low**—Specifies low sensitivity. • **medium**—Specifies medium sensitivity. • **high**—Specifies high sensitivity.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to set the high sensitivity for CleanAir event-driven RRM:

```
Device(config)# ap dot11 24ghz rrm channel cleanair-event sensitivity high
```

default ap dot11 24ghz cleanair device

To configure the default state of report generation for 2.4-GHz interference devices, use the **default ap dot11 24ghz cleanair device** command in global configuration mode.

Syntax Description

canopy	Configures the alarm for canopy interference devices.
cont-tx	Configures the alarm for continuous transmitters.
dect-like	Configures the alarm for Digital Enhanced Cordless Communication (DECT)-like phones.
inv	Configures the alarm for devices using spectrally inverted Wi-Fi signals.
jammer	Configures the alarm for jammer interference devices.
nonstd	Configures the alarm for devices using nonstandard Wi-Fi channels.
superag	Configures the alarm for 802.11 SuperAG interference devices.
tdd-tx	Configures the alarm for Time Division Duplex (TDD) transmitters.
video	Configures the alarm for video cameras.
wimax-fixed	Configures the alarm for WiMax fixed interference devices.
wimax-mobile	Configures the alarm for WiMax mobile interference devices.
report	Displays the device alarm report.
si_fhss	Specifies the QCA SI FHSS.

Command Default

The alarm for Wi-Fi inverted devices is enabled. The alarm for all other devices is disabled.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

You must enable CleanAir using the **ap dot11 24ghz cleanair**command before you configure this command.

This example shows how to enable CleanAir to report when a video camera interferes:

```
Device(config)# default ap dot11 24ghz cleanair device video
```

ap dot11 24ghz rrm channel cleanair-event

To enable Event-Driven RRM (EDRRM) and the sensitivity for 2.4-GHz devices, use the **ap dot11 24ghz rrm channel cleanair-event** command in global configuration mode. To disable EDRRM, use the **no** form of this command.

ap dot11 24ghz rrm channel cleanair-event sensitivity {**high** | **low** | **medium**}
no ap dot11 24ghz rrm channel cleanair-event [**sensitivity**{**high** | **low** | **medium**}]

Syntax Description

sensitivity	(Optional) Configures the EDRRM sensitivity of the CleanAir event.
high	(Optional) Specifies the highest sensitivity to non-Wi–Fi interference as indicated by the air quality (AQ) value.
low	(Optional) Specifies the least sensitivity to non-Wi–Fi interference as indicated by the AQ value.
medium	(Optional) Specifies medium sensitivity to non-Wi–Fi interference as indicated by the AQ value.

Command Default

EDRRM is disabled and the sensitivity is low.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

You must enable EDRRM using the **ap dot11 24ghz rrm channel cleanair-event** command before you configure the sensitivity.

This example shows how to enable EDRRM and set the EDRRM sensitivity to low:

```
Device(config)# ap dot11 24ghz rrm channel cleanair-event
Device(config)# ap dot11 24ghz rrm channel cleanair-event sensitivity low
```

ap dot11 24ghz rrm channel device

To configure persistent non-Wi-Fi device avoidance in the 802.11b channel, use the **ap dot11 24ghz rrm channel device** command in global configuration mode. To disable persistent device avoidance, use the **no** form of this command.

ap dot11 24ghz rrm channel device
no ap dot11 24ghz rrm channel device

Syntax Description

This command has no arguments or keywords.

Command Default

Persistent device avoidance is disabled.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

CleanAir-capable monitor mode access points collect information about persistent devices on all configured channels and stores the information in the switch. Local and bridge mode access points detect interference devices on the serving channels only.

This example shows how to enable persistent device avoidance:

```
Device(config)# ap dot11 24ghz rrm channel device
```

ap dot11 24ghz rrm optimized-roam

To configure optimized roaming for 802.11b network, use the **ap dot11 24ghz rrm optimized-roam** command.

ap dot11 24ghz rrm optimized-roam [**data-rate-threshold** {**11M** | **12M** | **18M** | **1M** | **24M** | **2M** | **36M** | **48M** | **54M** | **5_5M** | **6M** | **9M** | **disable**}]

Syntax Description

data-rate-threshold	Configures the data rate threshold for 802.11b optimized roaming.
11M	Sets the data rate threshold for 802.11b optimized roaming to 11 Mbps
12M	Sets the data rate threshold for 802.11b optimized roaming to of 12 Mbps
18M	Sets the data rate threshold for 802.11b optimized roaming to of 18 Mbps
1M	Sets the data rate threshold for 802.11b optimized roaming to of 1 Mbps
24M	Sets the data rate threshold for 802.11b optimized roaming to of 24 Mbps
2M	Sets the data rate threshold for 802.11b optimized roaming to of 2 Mbps
36M	Sets the data rate threshold for 802.11b optimized roaming to of 36 Mbps
48M	Sets the data rate threshold for 802.11b optimized roaming to of 48 Mbps
54M	Sets the data rate threshold for 802.11b optimized roaming to of 54 Mbps
5_5M	Sets the data rate threshold for 802.11b optimized roaming to of 5.5 Mbps
6M	Sets the data rate threshold for 802.11b optimized roaming to of 6 Mbps
9M	Sets the data rate threshold for 802.11b optimized roaming to of 9 Mbps
disable	Disables the data rate threshold.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure optimized roaming for 802.11b network:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 24ghz rrm optimized-roam
```

ap dot11 24ghz rx-sop threshold

To configure 802.11b radio receiver start-of-packet (RxSOP), use the **ap dot11 24ghz rx-sop threshold** command.

ap dot11 24ghz rx-sop threshold {**auto** | **high** | **low** | **medium** | **custom** *rxsop-value*}

Syntax Description

auto	Reverts RxSOP value to the default value.
high	Sets the RxSOP value to high threshold (–79 dBm).
medium	Sets the RxSOP value to medium threshold (–82 dBm).
low	Sets the RxSOP value to low threshold (–85 dBm).
custom *rxsop-value*	Sets the RxSOP value to custom threshold (–85 dBm to –60 dBm)

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

RxSOP determines the Wi-Fi signal level in dBm at which an access point's radio demodulates and decodes a packet. Higher the level, less sensitive the radio is and smaller the receiver cell size. The table below shows the RxSOP threshold values for high, medium, low, and custom levels for 2.4-GHz band.

Table 4: RxSOP Thresholds for 2.4-GHz Band

High Threshold	Medium Threshold	Low Threshold	Custom Threshold
–79 dBm	–82 dBm	–85 dBm	–85 dBm to –60 dBm

Examples

The following example shows how to configure 802.11b radio receiver start-of-packet (RxSOP) value to auto:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 24ghz rx-sop threshold auto
```

ap dot11 24ghz shutdown

To disable 802.11a network, use the **ap dot11 24ghz shutdown** command.

ap dot11 24ghz shutdown

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to disable the 802.11a network:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 24ghz shutdown
```

ap dot11 5ghz channelswitch quiet

To configure the 802.11h channel switch quiet mode, use the **ap dot11 5ghz channelswitch quiet** command.

ap dot11 5ghz channelswitch quiet

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the 802.11h channel switch quiet mode:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 5ghz channelswitch quiet
```

ap dot11 5ghz cleanair

To enable CleanAir for detecting 5-GHz devices, use the **ap dot11 5ghz cleanair** command in global configuration mode.

ap dot11 5ghz cleanair

Command Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

You must enable this CleanAir command before you configure other CleanAir commands.

This example shows how to enable CleanAir for 5-GHz devices:

```
Device(config)# ap dot11 5ghz cleanair
```

default ap dot11 5ghz cleanair device

To configure the default state of the alarm for 5-GHz interference devices, use the **default ap dot11 5ghz cleanair device** command in global configuration mode.

default ap dot11 5ghz cleanair device {**canopy** | **cont-tx** | **dect-like** | **inv** | **jammer** | **nonstd** | **radar** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile**}

Syntax Description

canopy	Configures the alarm for canopy interference devices.
cont-tx	Configures the alarm for continuous transmitters.
dect-like	Configures the alarm for Digital Enhanced Cordless Communication (DECT)-like phones.
inv	Configures the alarm for devices using spectrally inverted Wi-Fi signals.
jammer	Configures the alarm for jammer interference devices.
nonstd	Configures the alarm for devices using nonstandard Wi-Fi channels.
radar	Configures the alarm for radars.
report	Enables interference device reports.
superag	Configures the alarm for 802.11 SuperAG interference devices.
tdd-tx	Configures the alarm for Time Division Duplex (TDD) transmitters.
video	Configures the alarm for video cameras.
wimax-fixed	Configures the alarm for WiMax fixed interference devices.
wimax-mobile	Configures the alarm for WiMax mobile interference devices.

Command Default

The alarm for Wi-Fi inverted devices is enabled. The alarm for all other interference devices is disabled.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

You must enable CleanAir using the **ap dot11 5ghz cleanair** command before you configure this command.

This example shows how to enable CleanAir to report when a video camera interferes:

```
Device(config)# default ap dot11 5ghz cleanair device video
```

ap dot11 5ghz power-constraint

To configure the 802.11h power constraint value, use the **ap dot11 5ghz power-constraint** command. To remove the 802.11h power constraint value, use the **no** form of this command.

ap dot11 5ghz power-constraint *value*
no ap dot11 5ghz power-constraint

Syntax Description

value	802.11h power constraint value. **Note** The range is from 0 to 30 dBm.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure the 802.11h power constraint to 5 dBm:

```
Device(config)# ap dot11 5ghz power-constraint 5
```

ap dot11 5ghz rate

To configure 802.11a operational rates, use the **ap dot11 5ghz rate** command.

ap dot11 5ghz rate {**RATE_12M** | **RATE_18M** | **RATE_24M** | **RATE_36M** | **RATE_48M** | **RATE_54M** | **RATE_6M** | **RATE_9M**} {**disable** | **mandatory** | **supported**}

Syntax Description

RATE_12M	Configures the data to be transmitted at the rate of 12 Mbps
RATE_18M	Configures the data to be transmitted at the rate of 18 Mbps
RATE_24M	Configures the data to be transmitted at the rate of 24 Mbps
RATE_36M	Configures the data to be transmitted at the rate of 36 Mbps
RATE_48M	Configures the data to be transmitted at the rate of 48 Mbps
RATE_54M	Configures the data to be transmitted at the rate of 54 Mbps
RATE_6M	Configures the data to be transmitted at the rate of 6 Mbps
RATE_9M	Configures the data to be transmitted at the rate of 9 Mbps
disable	Disables the data rate that you specify. Also defines that the clients specify the data rates used for communication.
mandatory	Defines that the clients support this data rate in order to associate with an AP.
supported	Any associated clients support this data rate can communicate with the AP using this rate. However, the clients are not required to use this rate to associate with the AP.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Examples

The following example shows how to configure 802.11a operational rate to 24 Mbps and make it supported:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 5ghz rate RATE_24M supported
```

ap dot11 5ghz rrm channel cleanair-event

To enable Event-Driven RRM (EDRRM) and configure the sensitivity for 5-GHz devices, use the **ap dot11 5ghz rrm channel cleanair-event** command in global configuration mode. To disable EDRRM, use the **no** form of the command.

ap dot11 5ghz rrm channel cleanair-event [**sensitivity** {**high** | **low** | **medium**}]
no ap dot11 5ghz rrm channel cleanair-event [**sensitivity** {**high** | **low** | **medium**}]

Syntax Description

sensitivity	(Optional) Configures the EDRRM sensitivity of the CleanAir event.
high	(Optional) Specifies the highest sensitivity to non-Wi–Fi interference as indicated by the air quality (AQ) value.
low	(Optional) Specifies the least sensitivity to non-Wi–Fi interference as indicated by the AQ value.
medium	(Optional) Specifies medium sensitivity to non-Wi–Fi interference as indicated by the AQ value.

Command Default

EDRRM is disabled and the EDRRM sensitivity is low.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

You must enable EDRRM using the **ap dot11 5ghz rrm channel cleanair-event** command before you configure the sensitivity.

This example shows how to enable EDRRM and set the EDRRM sensitivity to high:

```
Device(config)# ap dot11 5ghz rrm channel cleanair-event
Device(config)# ap dot11 5ghz rrm channel cleanair-event sensitivity high
```

ap dot11 5ghz rrm channel device

To configure persistent non-Wi-Fi device avoidance in the 802.11a channel, use the **ap dot11 5ghz rrm channel device** command in global configuration mode. To disable persistent device avoidance, use the **no** form of this command.

ap dot11 5ghz rrm channel device
no ap dot11 5ghz rrm channel device

Syntax Description

This command has no arguments or keywords.

Command Default

The CleanAir persistent device state is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

CleanAir-capable monitor mode access points collect information about persistent devices on all configured channels and stores the information in the switch. Local and bridge mode access points detect interference devices on the serving channels only.

This example shows how to enable persistent device avoidance on 802.11a devices:

```
Device(config)# ap dot11 5ghz rrm channel device
```

ap dot11 5ghz rx-sop threshold

To configure 802.11a radio receiver start-of-packet (RxSOP), use the **ap dot11 5ghz rx-sop threshold** command.

ap dot11 5ghz rx-sop threshold {**auto** | **high** | **low** | **medium** | **custom** *rxsop-value*}

Syntax Description

auto	Reverts RxSOP value to the default value.
high	Sets the RxSOP value to high threshold (–76 dBm).
medium	Sets the RxSOP value to medium threshold (–78 dBm).
low	Sets the RxSOP value to low threshold (–80 dBm).
custom *rxsop-value*	Sets the RxSOP value to custom threshold (–85 dBm to –60 dBm)

Command Default

None

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

RxSOP determines the Wi-Fi signal level in dBm at which an access point's radio demodulates and decodes a packet. Higher the level, less sensitive the radio is and smaller the receiver cell size. The table below shows the RxSOP threshold values for high, medium, low, and custom levels for 5-GHz band.

Table 5: RxSOP Thresholds for 5-GHz Band

High Threshold	Medium Threshold	Low Threshold	Custom Threshold
–76 dBm	–78 dBm	–80 dBm	–85 dBm to –60 dBm

Examples

The following example shows how to configure 802.11b radio receiver start-of-packet (RxSOP) value to a custom value of –70 dBm:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 24ghz rx-sop threshold custom -70
```

ap dot11 5ghz shutdown

To disable 802.11a network, use the **ap dot11 5ghz shutdown** command.

ap dot11 5ghz shutdown

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to disable the 802.11a network:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 5ghz shutdown
```

ap dot11 5ghz smart-dfs

To configure to use nonoccupancy time for radar interference channel, use the **ap dot11 5ghz smart-dfs** command.

ap dot11 5ghz smart-dfs

Command Default None

Command Modes config

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Examples

The following example shows how to configure to use nonoccupancy time for radar interference channel:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 5ghz smart-dfs
```

ap dot11 beaconperiod

To change the beacon period globally for 2.4 GHz or 5 GHz bands, use the **ap dot11 beaconperiod** command.

Note Disable the 802.11 network before using this command. See the "Usage Guidelines" section.

ap dot11 {**24ghz** | **5ghz**} **beaconperiod** *time*

Syntax Description

24ghz	Specifies the settings for 2.4 GHz band.
5ghz	Specifies the settings for 5 GHz band.
beaconperiod	Specifies the beacon for a network globally.
time	Beacon interval in time units (TU). One TU is 1024 microseconds. The range is from 20 to 1000.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

In Cisco wireless LAN 802.11 networks, all Cisco lightweight access point wireless LANs broadcast a beacon at regular intervals. This beacon notifies clients that the wireless service is available and allows the clients to synchronize with the lightweight access point.

Before you change the beacon period, make sure that you have disabled the 802.11 network by using the **ap dot11** {**24ghz | 5ghz**} **shutdown** command. After changing the beacon period, enable the 802.11 network by using the **no ap dot11** {**24ghz | 5ghz**} **shutdown** command.

This example shows how to configure the 5 GHZ band for a beacon period of 120 time units:

```
Device(config)# ap dot11 5ghz beaconperiod 120
```

ap dot11 cac media-stream

To configure media stream Call Admission Control (CAC) voice and video quality parameters for 2.4 GHz and 5 GHz bands, use the **ap dot11 cac media-stream** command.

ap dot11 {**24ghz** | **5ghz**} **cac media-stream multicast-direct** {**max-retry-percent** *retryPercent* | **min-client-rate**{**eighteen** | **eleven** | **fiftyFour** | **fivePointFive** | **fortyEight** | **nine** | **oneFifty** | **oneFortyFourPointFour** | **oneThirty** | **oneThirtyFive** | **seventyTwoPointTwo** | **six** | **sixtyFive** | **thirtySix** | **threeHundred** | **twelve** | **twentyFour** | **two** | **twoSeventy**}}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
multicast-direct	Specifies CAC parameters for multicast-direct media streams.
max-retry-percent	Specifies the percentage of maximum retries that are allowed for multicast-direct media streams.
retryPercent	Percentage of maximum retries that are allowed for multicast-direct media streams. **Note** The range is from 0 to 100.
min-client-rate	Specifies the minimum transmission data rate to the client for multicast-direct media streams (rate at which the client must transmit in order to receive multicast-direct unicast streams). If the transmission rate is below this 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.

min-client-rate	You can choose the following rates: • **eighteen** • **eleven** • **fiftyFour** • **fivePointFive** • **fortyEight** • **nine** • **one** • **oneFifty** • **oneFortyFourPointFour** • **oneThirty** • **oneThirtyFive** • **seventyTwoPointTwo** • **six** • **sixtyFive** • **thirtySix** • **threeHundred** • **twelve** • **twentyFour** • **two** • **twoSeventy**

Command Default

The default value for the maximum retry percent 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 will be demoted for better effort QoS or is subject to denial.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **wlan** *wlan_name* **shutdown** command.

- Disable the radio network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **shutdown** command.
- Save the new configuration.
- Enable voice or video CAC for the network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **cac voice acm** or **ap dot11** {**24ghz | 5ghz**} **cac video acm** commands.

This example shows how to configure the maximum retry percent for multicast-direct media streams as 90 on a 802.11a network:

```
Device(config)# ap dot11 5ghz cac media-stream multicast max-retry-percent 90
```

ap dot11 cac multimedia

To configure multimedia Call Admission Control (CAC) voice and video quality parameters for 2.4 GHz and 5 GHz bands, use the **ap dot11 cac multimedia** command.

ap dot11 {**24ghz** | **5ghz**} **cac multimedia max-bandwidth** *bandwidth*

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
max-bandwidth	Specifies the percentage of maximum bandwidth allocated to Wi-Fi Multimedia (WMM) clients for voice and video applications on the 2.4 GHz or 5 GHz band.
bandwidth	Percentage of the maximum bandwidth allocated to WMM clients for voice and video applications on the 802.11a or 802.11b/g network. Once the client reaches the specified value, the access point rejects new multimedia flows this radio band. The range is from 5 to 85%.

Command Default

The default value is 75%.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **wlan** *wlan_name* **shutdown** command.
- Disable the radio network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **shutdown** command.
- Save the new configuration.
- Enable voice or video CAC for the network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **cac voice acm** or **ap dot11** {**24ghz | 5ghz**} **cac video acm** commands.

This example shows how to configure the percentage of the maximum bandwidth allocated to WMM clients for voice and video applications on the 5 GHz band:

```
Device(config)# ap dot11 5ghz cac multimedia max-bandwidth 5
```

ap dot11 cac voice

To configure Call Admission Control (CAC) parameters for the voice category, use the **ap dot11 cac voice** command.

ap dot11 {**24ghz** | **5ghz**} **cac voice** {**acm** | **load-based** | **max-bandwidth** *value* | **roam-bandwidth** *value* | **sip** [**bandwidth** *bw*] **sample-interval** *value* | **stream-size** *x* **max-streams** *y* | **tspec-inactivity-timeout** {**enable** | **ignore**}}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
acm	Enables bandwidth-based voice CAC for the 2.4 GHz or 5 GHz band. **Note** To disable bandwidth-based voice CAC for the 2.4 GHz or 5 GHz band, use the **no ap dot11** {**24ghz	5ghz**} **cac voice acm** command.
load-based	Enable load-based CAC on voice access category. **Note** To disable load-based CAC on voice access category for the 2.4 GHz or 5 GHz band, use the **no ap dot11** {**24ghz	5ghz**} **cac voice load-based** command.
max-bandwidth	Sets the percentage of the maximum bandwidth allocated to clients for voice applications on the 2.4 GHz or 5 GHz band.
value	Bandwidth percentage value from 5 to 85%.
roam-bandwidth	Sets the percentage of the CAC maximum allocated bandwidth reserved for roaming voice clients on the 2.4 GHz or 5 GHz band.
value	Bandwidth percentage value from 0 to 85%.
sip	Specifies the CAC codec name and sample interval as parameters and calculates the required bandwidth per call for the 802.11 networks.

bw	Bandwidth in kbps. The following bandwidth values specify parameters for the SIP codecs: • 64kbps—Specifies CAC parameters for the SIP G711 codec. • 8kbps—Specifies CAC parameters for the SIP G729 codec. **Note** The default value is 64 Kbps.
sample-interval	Specifies the packetization interval for SIP codec.
value	Packetization interval in msecs. The sample interval for SIP codec value is 20 seconds.
stream-size	Specifies the number of aggregated voice Wi-Fi Multimedia (WMM) traffic specification (TSPEC) streams at a specified data rate for the 2.4 GHz or 5 GHz band.
x	Stream size. The range of the stream size is from 84000 to 92100.
max-streams	Specifies the maximum number of streams per TSPEC.
y	Number (1 to 5) of voice streams. **Note** The default number of streams is 2 and the mean data rate of a stream is 84 kbps.
tspec-inactivity-timeout	Specifies TSPEC inactivity timeout processing mode. **Note** Use this keyword to process or ignore the Wi-Fi Multimedia (WMM) traffic specifications (TSPEC) inactivity timeout received from an access point. When the inactivity timeout is ignored, a client TSPEC is not deleted even if the access point reports an inactivity timeout for that client.
enable	Processes the TSPEC inactivity timeout messages.
ignore	Ignores the TSPEC inactivity timeout messages. **Note** The default is **ignore** (disabled).

Command Default None

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **wlan** *wlan_name* **shutdown** command.
- Disable the radio network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **shutdown** command.
- Save the new configuration.
- Enable voice or video CAC for the network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **cac voice acm** or **ap dot11** {**24ghz | 5ghz**} **cac video acm** commands.

This example shows how to enable the bandwidth-based CAC:

```
Device(config)# ap dot11 24ghz cac voice acm
```

This example shows how to enable the load-based CAC on the voice access category:

```
Device(config)# ap dot11 24ghz cac voice load-based
```

This example shows how to specify the percentage of the maximum allocated bandwidth for voice applications on the selected radio band:

```
Device(config)# ap dot11 24ghz cac voice max-bandwidth 50
```

This example shows how to configure the percentage of the maximum allocated bandwidth reserved for roaming voice clients on the selected radio band:

```
Device(config)# ap dot11 24ghz cac voice roam-bandwidth 10
```

This example shows how to configure the bandwidth and voice packetization interval for the G729 SIP codec on a 2.4 GHz band:

```
Device(config)# ap dot11 24ghz cac voice sip bandwidth 8 sample-interval 40
```

This example shows how to configure the number of aggregated voice traffic specifications stream with a stream size of 85000 and with a maximum of 5 streams:

```
Device(config)# ap dot11 24ghz cac voice stream-size 85000 max-streams 5
```

This example shows how to enable the voice TSPEC inactivity timeout messages received from an access point:

```
Device(config)# ap dot11 24ghz cac voice tspec-inactivity-timeout enable
```

ap dot11 cleanair

To configure CleanAir on 802.11 networks, use the **ap dot11 cleanair** command. To disable CleanAir on 802.11 networks, use the **no** form of this command.

ap dot11 {**24ghz** | **5ghz**} **cleanair**
no ap dot11 {**24ghz** | **5ghz**} **cleanair**

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
cleanair	Specifies CleanAir on the 2.4 GHz or 5 GHz band.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to enable the CleanAir settings on the 2.4 GHz band:

```
Device(config)# ap dot11 24ghz cleanair
```

ap dot11 cleanair device

To configure CleanAir interference device types, use the **ap dot11 cleanair device** command.

ap dot11 24ghz cleanair device [{**canopy** | **cont-tx** | **dect-like** | **inv** | **jammer** | **nonstd** | **report** | **si_fhss** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile**}]

Syntax Description

canopy	Specifies the Canopy devices.
cont-tx	Specifies the continuous transmitter.
dect-like	Specifies a Digital Enhanced Cordless Communication (DECT)-like phone.
inv	Specifies the devices using spectrally inverted Wi-Fi signals.
jammer	Specifies the jammer.
nonstd	Specifies the devices using nonstandard Wi-Fi channels.
superag	Specifies 802.11 SuperAG devices.
tdd-tx	Specifies the TDD transmitter.
video	Specifies video cameras.
wimax-fixed	Specifies a WiMax fixed device.
wimax-mobile	Specifies a WiMax mobile device.
report	Displays the device alarm report.
si_fhss	Specifies the QCA SI FHSS.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure the switch to monitor ZigBee interferences:

```
Device(config)# ap dot11 24ghz cleanair device report
```

ap dot11 dot11n

To configure settings for an 802.11n network, use the **ap dot11 dot11n** command.

ap dot11 {**24ghz** | **5ghz**} **dot11n** {**a-mpdu tx priority** {*priority_value* **all** } | **scheduler timeout rt** *scheduler_value*} | **a-msdu tx priority** {*priority_value* | **all**} | **guard-interval** {**any** | **long**} | **mcs tx** *rate* | **rifs rx**}

Syntax Description

24ghz	Specifies the 2.4-GHz band.
5ghz	Specifies the 5-GHz band.
dot11n	Enables 802.11n support.
a-mpdu tx priority	Specifies the traffic that is associated with the priority level that uses Aggregated MAC Protocol Data Unit (A-MPDU) transmission.
priority_value	Aggregated MAC protocol data unit priority level from 0 to 7.
all	Specifies all of the priority levels at once.
a-msdu tx priority	Specifies the traffic that is associated with the priority level that uses Aggregated MAC Service Data Unit (A-MSDU) transmission.
priority_value	Aggregated MAC protocol data unit priority level from 0 to 7.
all	Specifies all of the priority levels at once.
scheduler_value	The 802.11n A-MPDU transmit aggregation scheduler timeout value from 1 to 10000 milliseconds.
guard-interval	Specifies the guard interval.
any	Enables either a short or a long guard interval.
long	Enables only a long guard interval.
mcs tx *rate*	Specifies the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client.
rate	Specifies the modulation and coding scheme data rates. **Note** The range is from 0 to 23.
rifs rx	Specifies the Reduced Interframe Space (RIFS) between data frames.

Command Default By default, priority 0 is enabled.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines Aggregation is the process of grouping packet data frames together rather than transmitting them separately. The two aggregation methods available are:

- A-MPDU—This aggregation is performed in the software.
- A-MSDU—This aggregation is performed in the hardware

Aggregated MAC Protocol Data Unit priority levels assigned per traffic type are as follows:

- 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 10-ms latency and jitter
- 7—Network control
- all—Configure all of the priority levels at once.

Note Configure the priority levels to match the aggregation method used by the clients.

This example shows how to enable 802.11n support on a 2.4-GHz band:

```
Device(config)# ap dot11 24ghz dot11n
```

This example shows how to configure all the priority levels at once so that the traffic that is associated with the priority level uses A-MSDU transmission:

```
Device(config)# ap dot11 24ghz dot11n a-msdu tx priority all
```

This example shows how to enable only long guard intervals:

```
Device(config)# ap dot11 24ghz dot11n guard-interval long
```

This example shows how to specify MCS rates:

```
Device(config)# ap dot11 24ghz dot11n mcs tx 5
```

This example shows how to enable RIFS:

```
Device(config)# ap dot11 24ghz dot11n rifs rx
```

ap dot11 dtpc

To configure Dynamic Transmit Power Control (DTPC) settings, Cisco Client eXtension (CCX) version 5 expedited bandwidth request feature, and the fragmentation threshold on an 802.11 network, use the **ap dot11 dtpc** command.

ap dot11 {**24ghz** | **5ghz**} {**dtpc** | **exp-bwreq** | **fragmentation** *threshold*}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
dtpc	Specifies Dynamic Transport Power Control (DTPC) settings. **Note** This option is enabled by default.
exp-bwreq	Specifies Cisco Client eXtension (CCX) version 5 expedited bandwidth request feature. **Note** The expedited bandwidth request feature is disabled by default.
fragmentation *threshold*	Specifies the fragmentation threshold. **Note** This option can only used be when the network is disabled using the **ap dot11** {**24ghz	5ghz**} **shutdown** command.
threshold	Threshold. The range is from 256 to 2346 bytes (inclusive).

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

When the CCX version 5 expedited bandwidth request feature is enabled, the switch configures all joining access points for this feature.

This example shows how to enable DTPC for the 5 GHz band:

```
Device(config)# ap dot11 5ghz dtpc
```

This example shows how to enable the CCX expedited bandwidth settings:

```
Device(config)# ap dot11 5ghz exp-bwrep
```

This example shows how to configure the fragmentation threshold on the 5 GHz band with the threshold number of 1500 bytes:

```
Device(config)# ap dot11 5ghz fragmentation 1500
```

ap dot11 edca-parameters

To enable a specific enhanced distributed channel access (EDCA) profile on the 2.4 GHz or 5 GHz bands, use the **ap dot11 edca-parameters** command. To disable an EDCA profile on the 2.4 GHz or 5 GHz bands, use the **no** form of this command.

ap dot11 { **24ghz** | **5ghz** } **edca-parameters** { **client-load-based** | **custom-voice** | **optimized-video-voice** | **optimized-voice** | **svp-voice** | **wmm-default** }
no ap dot11 { **24ghz** | **5ghz** } **edca-parameters** { **client-load-based** | **custom-voice** | **fastlane** | **optimized-video-voice** | **optimized-voice** | **svp-voice** | **wmm-default** }

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
edca-parameters	Specifies a specific enhanced distributed channel access (EDCA) profile on the 802.11 networks.
fastlane	Enables Fastlane parameters for 24GHz.
client-load-based	Enables client load-based EDCA configuration for 802.11 radios.
custom-voice	Enables custom voice EDCA parameters.
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.
optimized-voice	Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than SpectraLink are 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.
wmm-default	Enables the Wi-Fi Multimedia (WMM) default parameters. Choose this option when voice or video services are not deployed on your network.

Command Default

wmm-default

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.
10.3	The **custom-voice** keyword was removed for Cisco 5700 Series WLC.
Cisco IOS XE Bengaluru 17.5.1	The **client-load-based** keyword was added.

This example shows how to enable SpectraLink voice priority parameters:

```
Device(config)# ap dot11 24ghz edca-parameters svp-voice
```

ap dot11 load-balancing denial

To configure the load balancing denial count, use the **ap dot11 load-balancingdenial**command. To disable load balancing denial count, use the **no** form of the command.

ap dot11 {**24ghz** | **5ghz**} **load-balancingdenial** *count*

Syntax Description

count	Load balancing denial count.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Example

The following example shows how to configure the load balancing denial count:

```
Device# configure terminal
Device(config)# ap dot11 5ghz load-balancing denial 10
```

ap dot11 load-balancing window

To configure the number of clients for the aggressive load balancing client window, use the **ap dot11 load-balancingwindow**command. To disable the client count, use the **no** form of the command.

ap dot11 {**24ghz** | **5ghz**} **load-balancingwindow** *clients*

Syntax Description

clients	Number of clients. Valid range is from 0 to 20.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Example

The following example shows how to configure the number of clients for the aggressive load balancing client window:

```
Device# configure terminal
Device(config)# ap dot11 5ghz load-balancing window 10
```

ap dot11 rf-profile

To configure an RF-Profile for a selected band, use the **ap dot11 rf-profile** command. To delete an RF-Profile, use the **no** form of this command.

ap dot11 {**24GHz** | **5GHz**} **rf-profile** *profile name*

Syntax Description

24ghz	Displays the 2.4-GHz band
5ghz	Displays the 5-GHz band
profile name	Name of the RF profile

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

None

This example shows how to configure an RF profile for a selected band.

```
Device#ap dot11 24GHz rf-profile doctest
```

ap dot11 rrm

To configure basic and advanced radio resource management settings for 802.11 devices, use the **ap dot11 rrm** command.

ap dot11 {**24ghz** | **5ghz**} **rrm** {**ccx location-measurement** *sec* | **channel** {**cleanair-event** | **dca** | **device** | **foreign** | **load** | **noise** | **outdoor-ap-dca**} | **coverage** {**data fail-percentage** *pct* | **data packet-count** *count* | **data rssi-threshold** *threshold*} | **exception global** *percentage* | **level global** *number* | **voice** {**fail-percentage** *percentage* | **packet-count** *number* | **rssi-threshold** *threshold*}}

Syntax Description

ccx	Configures Advanced (RRM) 802.11 CCX options.
location-measurement	Specifies 802.11 CCX Client Location Measurements in seconds. The range is between 10 and 32400 seconds.
channel	Configure advanced 802.11-channel assignment parameters.
cleanair-event	Configures cleanair event-driven RRM parameters.
dca	Configures 802.11-dynamic channel assignment algorithm parameters.
device	Configures persistent non-WiFi device avoidance in the 802.11-channel assignment.
foreign	Enables foreign AP 802.11-interference avoidance in the channel assignment.
load	Enables Cisco AP 802.11-load avoidance in the channel assignment.
noise	Enables non-802.11-noise avoidance in the channel assignment.
outdoor-ap-dca	Configures 802.11 DCA list option for outdoor AP.
coverage	Configures 802.11 coverage Hole-Detection.

data fail-percentage *pct*	Configures 802.11 coverage failure-rate threshold for uplink data packets. The range is between 1 and 100
data packet-count *count*	Configures 802.11 coverage minimum-failure-count threshold for uplinkdata packets.
data rssi-threshold *threshold*	Configures 802.11 minimum-receive-coverage level for voice packets.
exception global *percentage*	Configures 802.11 Cisco APs coverage-exception level. The range is between 0 and 100 percent.
level global *number*	Configures 802.11 Cisco AP client-minimum-exception level between 1 and 75 clients.
voice	Configures 802.11 coverage Hole-Detection for voice packets.
fail-percentage *percentage*	Configures 802.11 coverage failure rate threshold for uplink voice packets.
packet-count *number*	Configures 802.11 coverage minimum-uplink-failure count threshold for voice packets.
rssi-threshold *threshold*	Configures 802.11 minimum receive coverage level for voice packets.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

This command applies for both 802.11a and 802.11b bands. But the appropriate commands must be chosen for configuring the parameter.

This example shows how to configure various RRM settings.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm ?
```

```
ccx             Configure Advanced(RRM) 802.11a CCX options
channel         Configure advanced 802.11a channel assignment parameters
coverage        802.11a Coverage Hole Detection
group-member    Configure members in 802.11a static RF group
group-mode      802.11a RF group selection mode
logging         802.11a event logging
monitor         802.11a statistics monitoring
ndp-type        Neighbor discovery type Protected/Transparent
profile         802.11a performance profile
tpc-threshold   Configures the Tx Power Control Threshold used by RRM for auto
                power assignment
txpower         Configures the 802.11a Tx Power Level
```

ap dot11 rrm channel

To enable radio resource management channel for 2.4 GHz and 5GHz devices, use the **ap dot11 rrm channel** command. To disable the radio resource mangement for 2.4 GHz and 5 GHz devices, use the **no** form of the command.

ap dot11 {**24ghz** | **5ghz**} **rrm channel** {**cleanair-event** | **dca** | **device** | **foreign** | **load** | **noise**}
no ap dot11 {**24ghz** | **5ghz**} **rrm channel** {**cleanair-event** | **dca** | **device** | **foreign** | **load** | **noise**}

Syntax Description

cleanair-event	Specifies the cleanair event-driven RRM parameters
dca	Specifies the 802.11 dynamic channel assignment algorithm parameters
device	Specifies the persistent non-WiFi device avoidance in the 802.11-channel assignment.
foreign	Enables foreign AP 802.11-interference avoidance in the channel assignment.
load	Enables Cisco AP 802.11-load avoidance in the channel assignment.
noise	Enables non-802.11-noise avoidance in the channel assignment.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

None.

This example shows all the parameters available for **Channel**.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 24ghz rrm channel ?
  cleanair-event  Configure cleanair event-driven RRM parameters
  dca             Config 802.11b dynamic channel assignment algorithm
                  parameters
  device          Configure persistent non-WiFi device avoidance in the 802.11b
                  channel assignment
  foreign         Configure foreign AP 802.11b interference avoidance in the
                  channel assignment
  load            Configure Cisco AP 802.11b load avoidance in the channel
                  assignment
  noise           Configure 802.11b noise avoidance in the channel assignment
```

ap dot11 rrm channel dca

To configure Dynamic Channel Assignment (DCA) algorithm parameters on 802.11 networks, use the **ap dot11 rrm channel dca** command.

ap dot11 {**24ghz** | **5ghz**} **rrm channel dca**{**add** *value <1-14>* | **anchor-time** *value* | **global**{**auto** | **once**} | **interval** *value* | **min-metric** *value* | **remove** *value <1-14>* | **sensitivity**{**high** | **low** | **medium**}}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
add	Adds the 802.11b DCA channels to RRM allowed channel list
anchor-time	Specifies the anchor time for DCA.
value	Hour of time between 0 and 23. These values represent the hour from 12:00 a.m. to 11:00 p.m.
global	Specifies the global DCA mode for the access points in the 802.11 networks.
auto	Enables auto-RF.
once	Enables one-time auto-RF.
interval	Specifies how often the DCA is allowed to run.
value	Interval between the times when DCA is allowed to run. Valid values are 0, 1, 2, 3, 4, 6, 8, 12, or 24 hours. 0 is 10 minutes (600 seconds). Default value is 0 (10 minutes).
min-metric	Specifies the DCA minimum RSSI energy metric.
value	Minimum RSSI energy metric value from –100 to –60.
remove	Removes the 802.11b DCA channels from RRM allowed channel list.
sensitivity	Specifies how sensitive the DCA algorithm is to environmental changes (for example, signal, load, noise, and interference) when determining whether or not to change channels.
high	Specifies that the DCA algorithm is not particularly sensitive to environmental changes. See the “Usage Guidelines” section for more information.
low	Specifies that the DCA algorithm is moderately sensitive to environmental changes. See the “Usage Guidelines” section for more information.
medium	Specifies that the DCA algorithm is highly sensitive to environmental changes. See the “Usage Guidelines” section for more information.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

The DCA sensitivity thresholds vary by radio band as shown in the table below.

To aid in troubleshooting, the output of this command shows an error code for any failed calls. The table below explains the possible error codes for failed calls.

Table 6: DCA Sensitivity Threshold

Sensitivity	2.4 Ghz DCA Sensitivity Threshold	5 Ghz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

This example shows how to configure the switch to start running DCA at 5 pm for the 2.4 GHz band:

```
Device(config)# ap dot11 24ghz rrm channel dca anchor-time 17
```

This example shows how to set the DCA algorithm to run every 10 minutes for the 2.4 GHz band:

```
Device(config)# ap dot11 24ghz rrm channel dca interval 0
```

This example shows how to configure the value of DCA algorithm's sensitivity to low on the 2.4 GHz band:

```
Device(config)# ap dot11 24ghz rrm channel dca sensitivity low
```

ap dot11 rrm coverage

To enable 802.11 coverage hole detection, use the **ap dot11 rrm coverage** command.

ap dot11 {**24ghz** | **5ghz**} **rrm coverage** [{**data** {**fail-percentage** *percentage* | **packet-count** *count* | **rssi-threshold** *threshold*} | **exceptional global** *value* | **level global** *value* | **voice** {**fail-percentage** *percentage* | **packet-count** *packet-count* | **rssi-threshold** *threshold*}}]

Syntax Description

data	Specifies 802.11 coverage hole-detection data packets.
fail-percentage *percentage*	Specifies 802.11 coverage failure-rate threshold for uplink data packets. The range is between 1 and 100
packet-count *count*	Specifies 802.11 coverage minimum-failure-count threshold for uplink data packets.
rssi-threshold *threshold*	Specifies 802.11 minimum-receive-coverage level for voice packets.
exceptional global *value*	Specifies 802.11 Cisco APs coverage-exception level. The range is between 0 and 100 percent.
level global *value*	Specifies 802.11 Cisco AP client-minimum-exception level between 1 and 75 clients.
voice	Specifies 802.11 coverage Hole-Detection for voice packets.
fail-percentage *percentage*	Specifies 802.11 coverage failure rate threshold for uplink voice packets.
packet-count *packet-count*	Specifies 802.11 coverage minimum-uplink-failure count threshold for voice packets.
rssi-threshold *threshold*	Specifies 802.11 minimum receive coverage level for voice packets.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

If you enable coverage hole-detection, the switch automatically determines, based on data that is received from the access points, whether any access points have clients that are potentially located in areas with poor coverage.

If both the number and percentage of failed packets exceed the values that you entered in the **ap dot11 {24ghz | 5ghz} rrm coverage packet-count** and **ap dot11 {24ghz | 5ghz} rrm coverage fail-percentage** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The switch uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the

ap dot11 {24ghz | 5ghz} rrm coverage level-global and **ap dot11 {24ghz | 5ghz} rrm coverage exceptional-global** commands over a 90-second period. The switch determines whether the coverage hole can be corrected and, if appropriate, mitigate the coverage hole by increasing the transmit power level for that specific access point.

This example shows how to set the RSSI-threshold for data in 5-GHz band.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ap dot11 5ghz rrm coverage data rssi-threshold -80
```

ap dot11 rrm group-member

To configure members in an 802.11 static RF group, use the **ap dot11 rrm group-member** command. To remove members from 802.11 RF group, use the **no** form of this command.

ap dot11 {**24ghz** | **5ghz**} **rrm group-member** *controller-name controller-ip*
no ap dot11 {**24ghz** | **5ghz**} **rrm group-member** *controller-name controller-ip*

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
controller-name	Name of the switch to be added.
controller-ip	IP address of the switch to be added.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to add a switch in the 5 GHz band RF group:

```
Device(config)# ap dot11 5ghz rrm group-member cisco-controller 192.0.2.54
```

ap dot11 rrm group-mode

To set the 802.11 automatic RF group selection mode on, use the **ap dot11 rrm group-mode** command. To set the 802.11 automatic RF group selection mode off, use the **no** form of this command.

ap dot11 {**5ghz** | **24ghz**} **rrm group-mode** {**auto** | **leader** | **off**}
no ap dot11 {**5ghz** | **24ghz**} **rrm group-mode**

Syntax Description

5ghz	Specifies the 2.4 GHz band.
24ghz	Specifies the 5 GHz band.
auto	Sets the 802.11 RF group selection to automatic update mode.
leader	Sets the 802.11 RF group selection to static mode, and sets this switch as the group leader.
off	Sets the 802.11 RF group selection to off.

Command Default

auto

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to turn the auto RF group selection mode on the 5 GHz band:

```
Device(config)# ap dot11 5ghz rrm group-mode auto
```

ap dot11 rrm logging

To configure report log settings on supported 802.11 networks, use the **ap dot11 rrm logging** command.

ap dot11 {**24ghz** | **5ghz**} **rrm logging** {**channel** | **coverage** | **foreign** | **load** | **noise** | **performance** | **txpower**}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
channel	Turns the channel change logging mode on or off. The default mode is off (Disabled).
coverage	Turns the coverage profile logging mode on or off. The default mode is off (Disabled).
foreign	Turns the foreign interference profile logging mode on or off. The default mode is off (Disabled).
load	Turns the load profile logging mode on or off. The default mode is off (Disabled).
noise	Turns the noise profile logging mode on or off. The default mode is off (Disabled).
performance	Turns the performance profile logging mode on or off. The default mode is off (Disabled).
txpower	Turns the transit power change logging mode on or off. The default mode is off (Disabled).

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to turn the 5 GHz logging channel selection mode on:

```
Device(config)# ap dot11 5ghz rrm logging channel
```

This example shows how to turn the 5 GHz coverage profile violation logging selection mode on:

```
Device(config)# ap dot11 5ghz rrm logging coverage
```

This example shows how to turn the 5 GHz foreign interference profile violation logging selection mode on:

```
Device(config)# ap dot11 5ghz rrm logging foreign
```

This example shows how to turn the 5 GHz load profile logging mode on:

```
Device(config)# ap dot11 5ghz rrm logging load
```

This example shows how to turn the 5 GHz noise profile logging mode on:

```
Device(config)# ap dot11 5ghz rrm logging noise
```

This example shows how to turn the 5 GHz performance profile logging mode on:

```
Device(config)# ap dot11 5ghz rrm logging performance
```

This example shows how to turn the 5 GHz transmit power change mode on:

```
Device(config)# ap dot11 5ghz rrm logging txpower
```

ap dot11 rrm monitor

To Configure monitor settings on the 802.11 networks, use the **ap dot11 rrm monitor** command.

ap dot11 {**24ghz** | **5ghz**} **rrm monitor**{**channel-list** | {**all** | **country** | **dca**} | **coverage** | **load** | **noise** | **signal**} *seconds*

Syntax Description

24ghz	Specifies the 802.11b parameters.
5ghz	Specifies the 802.11a parameters.
channel-list all	Monitors the noise, interference, and rogue monitoring channel list for all channels.
channel-list country	Monitors the noise, interference, and rogue monitoring channel list for the channels used in the configured country code.
channel-list dca	Monitors the noise, interference, and rogue monitoring channel list for the channels used by automatic channel assignment.
coverage	Specifies the coverage measurement interval.
load	Specifies the load measurement interval.
noise	Specifies the noise measurement interval.
signal	Specifies the signal measurement interval.
rssi-normalization	Configure RRM Neighbor Discovery RSSI Normalization.
seconds	Measurement interval time from 60 to 3600 seconds.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to monitor the channels used in the configured country:

```
Device(config)# ap dot11 24ghz rrm monitor channel-list country
```

This example shows how to set the coverage measurement interval to 60 seconds:

```
Device(config)# ap dot11 24ghz rrm monitor coverage 60
```

ap dot11 rrm ndp-type

To configure the 802.11 access point radio resource management neighbor discovery protocol type, use the **ap dot11 rrm ndp-type** command.

ap dot11 {**24ghz** | **5ghz**} **rrm ndp-type** {**protected** | **transparent**}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
protected	Specifies the Tx RRM protected (encrypted) neighbor discovery protocol.
transparent	Specifies the Tx RRM transparent (not encrypted) neighbor discovery protocol.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

Before you configure the 802.11 access point RRM neighbor discovery protocol type, ensure that you have disabled the network by entering the **ap dot11** {**24ghz | 5ghz**} **shutdown** command.

This example shows how to enable the 802.11a access point RRM neighbor discovery protocol type as protected:

```
Device(config)# ap dot11 5ghz rrm ndp-type protected
```

ap dot11 24ghz rrm tpc

To configure the tx-power control threshold used by RRM for auto power assignment, use the **ap dot11 rrm tpc** command. To disable, use the **no** form of the command.

ap dot11 {**24ghz** | **5ghz**} **rrm tpc{threshold** | **tpcv1-chan-aware**}

Syntax Description

tpc threshold	Configures the Tx-Power Control threshold used by RRM..
tpcv1-chan-aware	Configures the Tx-Power Control to be channel aware.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None.

This example shows how to configure the tx-power control threshold used by RRM for auto power assignment.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 24ghz rrm tpc
```

ap dot11 rrm txpower

To configure the 802.11 tx-power level, use the **ap dot11 rrm txpower** command. To disable the 802.11 tx-power level, use the **no** form of the command.

ap dot11 {**24ghz** | **5ghz**} **rrm txpower** {*powerLevel <1-5>* | **auto** | **max** *powerLevel* | **min** *powerLevel* | **once***power-level*}

Syntax Description

powerLevel	Configures the transmit power level.
auto	Enables auto-RF.
max *powerLevel*	Configures maximum auto-RF tx power. The range is between -10 to -30.
min *powerLevel*	Configures minimum auto-RF tx power. The range is between -10 to -30.
once	Enables one-time auto-RF.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None.

This example shows how to enables auto-RF once.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm txpower once
```

ap dot11 rrm txpower

To configure the 802.11 tx-power level, use the **ap dot11 rrm txpower** command. To disable the 802.11 tx-power level, use the **no** form of the command.

ap dot11 {**24ghz** | **5ghz**} **rrm txpower** {*powerLevel <1-5>* | **auto** | **max** *powerLevel* | **min** *powerLevel* | **once***power-level*}

Syntax Description

powerLevel	Configures the transmit power level.
auto	Enables auto-RF.
max *powerLevel*	Configures maximum auto-RF tx power. The range is between -10 to -30.
min *powerLevel*	Configures minimum auto-RF tx power. The range is between -10 to -30.
once	Enables one-time auto-RF.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None.

This example shows how to enables auto-RF once.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm txpower once
```

ap filter

To configure the AP filter and set the priority, use the **ap filter** command.

ap filter { { **name***filter-name*} | {**priority** *priority-number* | **filter-name** *filter-name*} }

Syntax Description

Parameter	Description
priority	Set the priority for a name filter.
priority-number	The valid AP filter priority range is 0 to 127.
filter-name	Enter the name for the ap filter.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Examples

The following example shows how to create a ap filter and set the priority to this filter:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap filter namep-filter-name1
Device(config-aaa-policy)# aaa-realm enable
```

ap fra

To configure flexible radio assignment (FRA) and its parameters, use the **ap fra** command.

ap fra[{**interval** *no-of-hours* | **sensitivity** {**high** | **low** | **medium** } | **sensor-threshold** {**balanced** | **client-preferred** | **client-priority** | **sensor-preferred** | **sensor-priority** } | **service-priority** {**coverage** | **service-assurance**}}]

Syntax Description

interval *no-of-hours*	Enter the number of hours for the FRA interval. Valid range is 1 to 24 hours.
sensitivity {**high**	**low**	**medium**}	Configures the FRA coverage overlap sensitivity as high, low, or medium.
sensor-threshold {**balanced**	**client-preferred**	**client-priority**	**sensor-preferred**	**sensor-priority**}	Configures FRA sensor threshold to one of the available options.
service-priority {**coverage**	**service-assurance**}	Configures FRA service priority to Coverage or Service Assurance.

Command Default

None

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

Ensure that the RF group leader for 802.11b/g and 802.11a bands are same across RF domain and make sure that the RF group leader has FRA enabled.

Examples

The following example show how to configure the FRA interval to 8 hours:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap fra interval 8
```

ap image predownload

To instruct all APs to start image predownload, use the **ap image predownload** command.

ap image predownload {**abort** | **site-tag** *site-tag-name* **start**}

Syntax Description

abort	Instructs all the APs to abort image predownload.
site-tag	Initiates image predownload parameters.
site-tag-name	Specifies the site-tag name.
start	Starts image predownload.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

Example

This example shows how the APs are instructed to start image predownload:

```
Device#ap image download site-tag site-tag-name start
```

ap name antenna band mode

To configure the antenna mode, use the **ap name***ap- name* **antenna-band-mode{ single | dual }** command.

ap name*ap-name* **antenna-band-mode**{**single** | **dual**}

Syntax Description

ap- name	Name of the Cisco lightweight access point.
antenna-band-mode	Instructs the access point to enable the band mode of antenna.

Command Default

None

Example

This example shows how to configure the antenna band mode of access point.

```
Device ap name <ap-name> antenna-band-mode single
```

ap name ble

To enable the able ltx state on the AP, use the **ap name** *ap name* **ble** command.

ap name *ap_name* **antena-band-mode {admin | ibeacon | interval | no-advertisement | sync | vibeacon}**

Syntax Description

ap name	AP Name
admin	Enables the ble ltx admin state.
ibeacon	Enables the BLE LTX iBeacon configuration.
interval	Enables the BLE LTX scan configuration interval.
no-advertisement	Enables the BLE LTX No Advertisement.
Sync	Enables the BLE LTX synchronize.
vibeacon	Enables the BLE LTX viBeacon configuration.

Command Default

Disabled

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following example shows how to enable ble on the AP:

```
Device# ap name test ble
```

ap name clear-personal-ssid

To clear the personal SSID from a Cisco OfficeExtend Access Point (OEAP), use the **ap name clear-personal-ssid** command.

ap name *ap-name* **clear-personal-ssid**

Syntax Description

ap-name	AP name.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Examples

The following example shows how to clear the personal SSID from a Cisco OEAP:

```
Device# ap name my-oeap clear-personal-ssid
```

ap name controller

To configure the controller on the AP, use the **ap name** *ap name* **controller** command.

ap name *ap_name* **controller {primary | secondary | tertiary}** *name {A.B.C.D | X:X:X::XX}*

Syntax Description

ap name	AP Name
controller	Configures the controller.
primary	Configures the primary controller.
secondary	Configures the secondary controller.
tertiary	Configures the tertiary controller.
name	Specifies the name of the primary controller, secondary controller, or tertiary controller.
A.B.C.D	Specifies theIPv4 address of the primary controller, secondary controller, or tertiary controller.
X:X:X::XX	Specifies theIPv6 address of the primary controller, secondary controller, or tertiary controller.

Command Default

Disabled

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following example shows how to configure the controller on the AP:

```
Device# ap name cisco-ap controller primary cisco-primary-controller 10.1.1.1
```

ap name country

To configure the country of operation for a Cisco lightweight access point, use the **ap name country** command.

ap name *ap-name* **country** *country-code*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
country-code	Two-letter or three-letter country code.

Command Default

None

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

Cisco switchs must be installed by a network administrator or qualified IT professional and the installer must select the proper country code. Following installation, access to the unit should be password protected by the installer to maintain compliance with regulatory requirements and to ensure proper unit functionality. See the related product guide for the most recent country codes and regulatory domains. Also, access point regulatory domains are defined during the access point manufacturing process. You can change the access point country code if the new country code matches a country that is valid within the access point regulatory domain. If you try to enter a country that is not valid to the access point regulatory domain, the command fails.

This example shows how to configure the Cisco lightweight access point's country code to DE:

```
Device# ap name AP2 country JP
```

ap name crash-file

To manage crash data and radio core files for the Cisco access point, use the **ap name crash-file** command.

ap name *ap-name* **crash-file** {**get-crash-data** | **get-radio-core-dump** {**slot 0** | **slot 1**}}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
get-crash-data	Collects the latest crash data for a Cisco lightweight access point.
get-radio-core-dump	Gets a Cisco lightweight access point's radio core dump
slot	Slot ID for Cisco access point.
0	Specifies Slot 0.
1	Specifies Slot 1.

Command Default

None

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to collect the latest crash data for access point AP3:

```
Device# ap name AP3 crash-file get-crash-data
```

This example shows how to collect the radio core dump for access point AP02 and slot 0:

```
Device# ap name AP02 crash-file get-radio-core-dump slot 0
```

ap name dot11 24ghz slot 0 SI

To enable Spectrum Intelligence (SI) for the dedicated 2.4-GHz radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot 0 SI** command.

ap name *ap-name* **dot11** { **24ghz** | **5ghz** | **dual-band** | **rx-dual-band** } **slot** *slot ID* **SI**

Syntax Description

ap_name	Name of the Cisco Access Point.
slot 0	Enables Spectrum Intelligence (SI) for the dedicated 2.4-GHz radio hosted on slot 0 for a specific access point. Here, 0 refers to the Slot ID.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Example

The following example shows how to configure Spectrum Intelligence of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 SI
```

ap name dot11 24ghz slot antenna

To configure the 802.11b antenna hosted on slot 0, use the **ap name dot11 24ghz slot antenna** command.

ap name *ap-name***dot1124ghzslot 0antenna** { **ext-ant-gain** *antenna-gain-value* | **selection** [**internal** | **external** }

Syntax Description

ap-name	Name of the AP.
24ghz	Configures 802.11b parameters.
slot	Sets the slot ID for the Cisco Access Point.
antenna	Configures the 802.11b Antenna.
ext-ant-gain	Configures the 802.11b External Antenna Gain. The value range is 0 - 4294967295. Enter External Antenna Gain value in multiple of .5 dBi units (i.e. An integer value 4 means 4 x 0.5 = 2 dBi of gain)
selection	Configure the 802.11b Antenna selection (internal/external)

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

Example

The following example shows how to configure the channel width of an AP.

```
Device# ap name ax1 dot11 24ghz slot 0 antenna selection external
```

ap name dot11 24ghz slot beamforming

To configures beamforming for the 2.4-GHz radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot beamforming** command.

ap name *ap-name***dot1124ghzslot 0beamforming**

Syntax Description

beamforming	Enable 802.11b tx beamforming - 5 GHz

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

Example

The following example shows how to configure beamforming of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 beamforming
```

ap name dot11 24ghz slot channel

To configure advanced 802.11 channel assignment parameters for Cisco AP, use the **ap name dot11 24ghz slot channel** command.

ap name *ap-name* **dot11 24ghz slot 0 channel** { *channel_number* | **auto** }

Syntax Description

channel_number	Advanced 802.11 channel assignment parameters for Cisco AP. Enter a channel number from 1 - 14.
auto	Enables auto RF.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

Example

The following example shows how to configure the channel of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 channel auto
```

ap name dot11 24ghz slot cleanair

To enable CleanAir for 802.11b radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot cleanair** command.

ap name *ap-name* **dot11 24ghz slot 0 cleanair**

Syntax Description

cleanair	Enables 802.11b cleanair management

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Example

The following example shows how to configure the cleanair of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 cleanair
```

ap name dot11 24ghz slot dot11n antenna

To configure 802.11n antenna for 2.4-GHz radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot dot11n antenna** command.

ap name *ap-name* **dot11 24ghz slot 0 dot11n antenna** { **A** | **B** | **C** | **D** }

Syntax Description

dot11n	Configures 802.11n antenna for 2.4-GHz radio hosted on slot 0 for a specific access point.
antenna	Configures the 802.11n - 2.4 GHz antenna selection from antenna ports A, B, C, and D.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Example

The following example shows how to configure the channel width of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 dot11n antenna A
```

ap name dot11 24ghz slot dot11ax bss-color

To set the BSS color on the 2.4 GHz, 5 GHz, or dual-band radio, for a specific access point, use the **ap name dot11 24ghz slot dot11ax bss-color** command.

ap name *ap-name* **dot11 24ghz slot 0 dot11ax bss-color** *<1-63>*

Syntax Description

bss-color	Configures 802.11ax-2.4GHz BSS color

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Example

The following example shows how to disable 802.11b radio on Cisco AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 dot11ax bss-color 3
```

ap name dot11 24ghz slot shutdown

To disable 802.11b radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot shutdown** command.

ap name *ap-name* **dot11 24ghz slot 0 shutdown**

Syntax Description

shutdown	Disables 802.11b radio on Cisco AP

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Example

The following example shows how to disable 802.11b radio on Cisco AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 shutdown
```

ap name dot11 dual-band cleanair

To configure CleanAir for a dual band radio, use the **ap name dot11 dual-band cleanair** command.

ap name *ap-name* **dot11 dual-band cleanair**
ap name *ap-name* **no dot11 dual-band cleanair**

Syntax Description

ap-name	Name of the Cisco AP.
cleanair	Specifies the CleanAir feature.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to enable CleanAir for a dual band radio of the access point AP01:

```
Device# ap name AP01 dot11 dual-band cleanair
```

ap name dot11 dual-band shutdown

To disable dual band radio on a Cisco AP, use the **ap name dot11 dual-band shutdown** command.

ap name *ap-name* **dot11 dual-band shutdown**
ap name *ap-name* **no dot11 dual-band shutdown**

Syntax Description

ap-name	Name of the Cisco AP.
shutdown	Disables the dual band radio on the Cisco AP.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to disable dual band radio on the Cisco access point AP01:

```
Device# ap name AP01 dot11 dual-band shutdown
```

ap name dot11 rrm profile

To configure Radio Resource Management (RRM) performance profile settings for a Cisco lightweight access point, use the **ap name dot11 rrm profile** command.

ap name *ap-name* **dot11** {**24ghz** | **5ghz**} **rrm profile** {**clients** *value* | **customize** | **foreign** *value* | **noise** *value* | **throughput** *value* | **utilization** *value*}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
clients	Sets the access point client threshold.
value	Access point client threshold from 1 to 75 clients. **Note** The default client threshold is 12.
customize	Turns on performance profile customization for an access point. **Note** Performance profile customization is off by default.
foreign	Sets the foreign 802.11 transmitter interference threshold.
value	Foreign 802.11 transmitter interference threshold from 0 to 100 percent. **Note** The default is 10 percent.
noise	Sets the 802.11 foreign noise threshold.
value	802.11 foreign noise threshold between –127 and 0 dBm. **Note** The default is —70 dBm.
throughput	Sets the data-rate throughput threshold.
value	802.11 throughput threshold from 1000 to 10000000 bytes per second. **Note** The default is 1,000,000 bytes per second.
utilization	Sets the RF utilization threshold. **Note** The operating system generates a trap when this threshold is exceeded.
value	802.11 RF utilization threshold from 0 to 100 percent. **Note** The default is 80 percent.

Command Default None

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to set the AP1 clients threshold to 75 clients:

```
Device# ap name AP1 dot11 24ghz rrm profile clients 75
```

This example shows how to turn performance profile customization on for 802.11a Cisco lightweight access point AP1:

```
Device# ap name AP1 dot11 5ghz rrm profile customize
```

This example shows how to set the foreign 802.11a transmitter interference threshold for AP1 to 0 percent:

```
Device# ap name AP1 dot11 5ghz rrm profile foreign 0
```

This example shows how to set the 802.11a foreign noise threshold for AP1 to 0 dBm:

```
Device# ap name AP1 dot11 5ghz rrm profile noise 0
```

This example shows how to set the AP1 data-rate threshold to 10000000 bytes per second:

```
Device# ap name AP1 dot11 5ghz rrm profile throughput 10000000
```

This example shows how to set the RF utilization threshold for AP1 to 100 percent:

```
Device# ap name AP1 dot11 5ghz rrm profile utilization 100
```

ap name image

To configure an image on a specific access point, use the **ap name image** command.

ap name *ap-name* **image** {**predownload** | **swap**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
predownload	Instructs the access point to start the image predownload.
swap	Instructs the access point to swap the image.

Command Default

None

Command History

Release	Modification
	This command was introduced.

This example shows how to predownload an image to an access point:

```
Device# ap name AP2 image predownload
```

This example shows how to swap an access point's primary and secondary images:

```
Device# ap name AP2 image swap
```

ap name indoor

To enable the access point in the indoor mode, use the **ap name** *ap name* **indoor** command.

ap name *ap_name* **indoor**

Syntax Description

ap name	AP Name
indoor	Enables the access point in the indoor mode.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following example shows how to enable the access point in the indoor mode:

```
Device# ap name test indoor
```

ap name ipsla

To configure ipsla on the AP, use the **ap name** *ap name* **ipsla** command.

ap name *ap_name* **ipsla**

Syntax Description

ap name	AP Name
ipsla	Enables the ipsla on the access point.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following example shows how to configure ipsla on the access point:

```
Device# ap name test ipsla
```

ap name keepalive

To enable the keepalive option on the AP, use the **ap name** *ap name* **keepalive** command.

ap name *ap_name* **keepalive**

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 17.03.1	This command was introduced.

Examples

The following example shows how to enable the keepalive option on the AP:

```
Device# ap name test keepalive
```

ap name lan

To configure LAN port configurations for APs, use the **ap name lan** command. To remove LAN port configurations for APs, use the**ap name no lan** command.

ap name *ap-name* **[no]lan port-id** *port-id* {**shutdown** | **vlan-access**}

Syntax Description

no	Removes LAN port configurations.
port-id	Configures the port.
port-id	The ID of the port. The range is 1-4
shotdown	Disables the Port.
vlan-access	Enables VLAN access to Port.

Command Default

None

Command Modes

Privileged EXEC(#)

This example shows how to enable VLAN access to port:

```
Device# ap name AP1 lan port-id 1 vlan-access
```

ap name led

To enable the LED state for an access point, use the **ap name led** command. To disable the LED state for an access point, use the **no** form of this command.

ap name *ap-name* **led**
no ap name *ap-name* [**led**] **led**

Syntax Description

ap-name	Name of the Cisco lightweight access point.
led	Enables the access point's LED state.

Command Default

None

Command History

Release	Modification
	This command was introduced.

This example shows how to enable the LED state for an access point:

```
Device# ap name AP2 led
```

This example shows how to disable the LED state for an access point:

```
Device# ap name AP2 no led
```

ap name led-brightness-level

To configure the LED brightness level on the AP, use the **ap name** *ap name* **led-brightness-level** command.

ap name *ap_name* **led-brightness-level {1–8}**

Syntax Description

ap name	AP Name
led brightness level	Configures the led brightness level. **Note** Valid led brightness level is from 1 to 8.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following example shows the LED brightness level on the access point:

```
Device# ap name cisco-ap led-brightness-level2
```

ap name location

To modify the descriptive location of a Cisco lightweight access point, use the **ap name location** command.

ap name *ap-name* **location** *location*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
location	Location name of the access point (enclosed by double quotation marks).

Command Default

None

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

The Cisco lightweight access point must be disabled before changing this parameter.

This example shows how to configure the descriptive location for access point AP1:

```
Device# ap name AP1 location Building1
```

ap name mdsn-ap

To configure mdsn-ap on the AP, use the **ap name** *ap name* **mdsn-ap** command.

ap name *ap_name* **mdsn-ap {disable | enable | vlan}** *add delete*

Syntax Description

ap name	AP Name
disable	Disables the mDNS access point.
enable	Enables the mDNS access point.
vlan	Adds or deletes the VLAN from mDNS access point.
add	Adds vlan to mDNS AP.
add	Deletes vlan from the mDNS AP.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following example shows how to enable mdns on the AP:

```
Device# Device# ap name test mdns enable
```

ap name name new-ap-name

To configure the new Cisco AP name, use the **ap name** *ap name* **name** *new-ap-name* command.

ap name *ap_name* **name** *new-ap-name*

Syntax Description

ap name	AP Name
name	Specifies the new Cisco AP name.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following example shows how to configure the new Cisco AP:

```
Device# ap name test name test2
```

ap name no

To negate a command or set its defaults on the AP, use the **no** command.

ap name *ap_name* **no**

Syntax Description

ap name	AP Name
no	Negate a command or set its defaults.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following example shows how to negate a command or set its defaults on the AP:

```
Device# ap name test no
```

ap name monitor-mode dot11b

To configures 802.11b scanning channels for a monitor-mode access point, use the **ap name monitor-mode dot11b** command.

ap name *ap-name* **monitor-mode dot11b fast-channel** *channel1* [*channel2*] [*channel3*] [*channel4*]

Syntax Description

ap-name	Name of the access point.
fast-channel	Specifies the 2.4 GHz band scanning channel (or channels) for a monitor-mode access point.
channel1	Scanning channel1.
channel2	(Optional) Scanning channel2.
channel3	(Optional) Scanning channel3.
channel4	(Optional) Scanning channel4.

Command Default

None

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to configure an access point in tracking optimized mode to listen to channels 1, 6, and 11:

```
Device# ap name AP01 monitor-mode dot11b fast-channel 1 6 11
```

ap name name

To modify the name of a Cisco lightweight access point, use the **ap name name** command.

ap name *ap-name* **name** *new-name*

Syntax Description

ap-name	Current Cisco lightweight access point name.
new-name	Desired Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
	This command was introduced.

This example shows how to modify the name of access point AP1 to AP2:

```
Device# ap name AP1 name AP2
```

ap name priority

To configure the priority of an access point, use the **ap name priority** command.

ap name *ap-name* **priority** *priority-value*

Syntax Description

priority-value	Priority value for the AP. Valid range is 1 to 4.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Examples

The following example shows how to configure the priority for an access point:

```
Device# ap name my-ap priority 1
```

ap name reset

To reset a specific Cisco lightweight access point, use the **ap name reset** command.

ap name *ap-name* **reset**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
	This command was introduced.

This example shows how to reset a Cisco lightweight access point named AP2:

```
Device# ap name AP2 reset
```

ap name reset-button

To configure the Reset button for an access point, use the **ap name reset-button** command.

ap name *ap-name* **reset-button**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
	This command was introduced.

This example shows how to enable the Reset button for access point AP03:

```
Device# ap name AP03 reset-button
```

ap name role

To configure the role of operation for an AP, use the **ap name role** command.

ap name *ap-name* **role** {**mesh-ap** | **root-ap**}

Syntax Description

ap-name	Name of the AP.
mesh-ap	Configures mesh AP role for the AP.
root-ap	Configures root AP role for the AP.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Examples

The following example shows how to configure the role of operation as mesh AP for an AP:

```
Device# ap name mymeshap role mesh-ap
```

ap name slot

To configure various slot parameters, use the **ap name slot** command. To disable a slot on a Cisco lightweight access point, use the **no** form of this command.

ap name *ap-name* **slot** *slot-number* {**channel** {**global** | **number** *channel-number* | **width** *channel-width*} | **rtsthreshold** *value* | **shutdown** | **txpower** {**global***channel-level*}}
ap name *ap-name* **no slot** {**0** | **1** | **2** | **3**} **shutdown**

Syntax Description

ap-name	Name of the Cisco access point.
slot-number	Slot downlink radio to which the channel is assigned. You can specify the following slot numbers: • **0**—Enables slot number 0 on a Cisco lightweight access point. • **1**—Enables slot number 1 on a Cisco lightweight access point. • **2**—Enables slot number 2 on a Cisco lightweight access point. • **3**—Enables slot number 3 on a Cisco lightweight access point.
channel	Specifies the channel for the slot.
global	Specifies channel global properties for the slot.
number	Specifies the channel number for the slot.
channel-number	Channel number from 1 to 169.
width	Specifies the channel width for the slot.
channel-width	Channel width from 20 to 40.
rtsthreshold	Specifies the RTS/CTS threshold for an access point.
value	RTS/CTS threshold value from 0 to 65535.
shutdown	Shuts down the slot.
txpower	Specifies Tx power for the slot.
global	Specifies auto-RF for the slot.
channel-level	Transmit power level for the slot from 1 to 7.

Command Default

None

Command History

Release	Modification
	This command was introduced.

This example shows how to enable slot 3 for the access point abc:

```
Device# ap name abc slot 3
```

This example shows how to configure RTS for the access point abc:

```
Device# ap name abc slot 3 rtsthreshold 54
```

ap name static-ip

ap name *Cisco-ap-name***static-ipip-address** { **A.B.C.Dnetmask***netmask* | **X:X:X:X::Xprefix***prefix-length* } **gateway***gateway*

Syntax Description

ap name	Name of the Cisco access point.
static-ip	Sets the Cisco AP static IP address configuration.
ip-address	Adds the Cisco AP static IP address.
A.B.C.D	Indicates the IPv4 address.
X:X:X:X::X	Indicates the IPv6 address.
netmask*netmask*	Specifies the Cisco AP static-IP netmask.
prefix*prefix-length*	Specifies the Cisco AP static-IP prefix length.
gateway*gateway*	Specifies the Cisco AP static-IP gateway.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

The following example shows how to enable or disable static-ip for an access point:

```
Device#ap name cisco-ap-name static-ip ip-address 9.9.9.2 netmask 255.0.0.0 gateway 9.9.9.2
```

ap name static-ip

To configure lightweight access point static IP settings, use the **ap name static-ip** command. To disable the Cisco lightweight access point static IP address, use the **no** form of this command.

ap name *ap-name* **static-ip** {**domain** *domain-name* | **ip-address** *ip-address* **netmask** *netmask* **gateway** *gateway* | **nameserver** *ip-address*}
ap name *ap-name* **no static-ip**

Syntax Description

ap-name	Name of the access point.
domain	Specifies the Cisco access point domain name.
domain-name	Domain to which a specific access point belongs.
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.
nameserver	Specifies a DNS server so that a specific access point can discover the switch using DNS resolution.
ip-address	IP address of the DNS server.

Command Default

None

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

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.

This example shows how to configure an access point static IP address:

```
Device# ap name AP2 static-ip ip-address 192.0.2.54 netmask 255.255.255.0 gateway 192.0.2.1
```

ap name shutdown

To disable a Cisco lightweight access point, use the **ap name shutdown** command. To enable a Cisco lightweight access point, use the **no** form of this command.

ap name *ap-name* **shutdown**
ap name *ap-name* **no shutdown**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

This example how to disable a specific Cisco lightweight access point:

```
Device# ap name AP2 shutdown
```

ap name vlan-tag

To configure VLAN tagging for a nonbridge AP, use the **ap name vlan-tag** command.

ap name *ap-name* **vlan-tag** *vlan-id*

Syntax Description

ap-name	Access point name.
vlan-id	VLAN identifier.

Command Default

VLAN tagging is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Example

The following example shows how to configure VLAN tagging for a nonbridge AP:

```
Device# ap name AP1 vlan-tag 12
```

ap name write tag-config

To write the existing configuration to an AP, use the **ap name write tag-config** command in privileged EXEC mode

ap name *ap-name***write tag-config**

Syntax Description

ap-name	Name of the access point.

Command Default

None

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Usage Guidelines

Use this command to write the existing configuration to an AP.

Example

This example shows how to write the existing configuration to an AP:

```
Device# ap name AP40CE.2485.D594 write tag-config
```

ap name-regex

To configure filter based on AP name regular expression to match with, use the **ap name-regex** command.

ap name-regex *regular-expression*

Syntax Description

regular-expression	Enter the filter string.

Command Default

None

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Examples

The following example shows how to configure filter based on AP name regular expression match with:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap filter name filter--name
Device(config-ap-filter)# ap name-regex regular-expression-string
```

ap profile

To configure access point profile, use the **ap profile** command.

ap profile *profile-name*

Syntax Description

profile-name	Enter the name of the AP profile.

Command Default

By default, the AP profile name is default-ap-profile.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Examples

The following example shows how to configure AP profile name:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap profile my-ap-profile
```

ap remote-lan profile-name

To configure remote LAN profile, use the **ap remote-lan profile-name** command.

ap remote-lan profile-name *remote-lan-profile-name rlan-id*

Syntax Description

remote-lan-profile-name	Is the remote LAN profile name. Range is from 1 to 32 alphanumeric characters.
rlan-id	Is the remote LAN identifier. Range is from 1 to 128.

Note You can create a maximum of 128 RLANs. You cannot use the *rlan-id* of an existing RLAN while creating another RLAN.

Both RLAN and WLAN profile cannot have the same names. Similarly, RLAN and WLAN policy profile cannot have the same names.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to configure remote LAN profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap remote-lan profile-name rlan_profile_name 3
```

ap remote-lan shutdown

To enable or disable all RLANs, use the **ap remote-lan shutdown** command.

ap remote-lan shutdown

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Example

This example shows how to enable or disable all RLANs:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# [no] ap remote-lan shutdown
Device(config)# end
```

ap remote-lan-policy policy-name

To configure RLAN policy profile, use the **ap remote-lan-policy policy-name** command.

ap remote-lan-policy policy-name *profile-name*

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Example

This example shows how to configure RLAN policy profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap remote-lan-policy policy-name rlan_policy_prof_name
```

ap tag-source-priority

To configure ap tag source priority, use the **ap tag-source-priority** command.

ap tag-source-priority *source-priority* **source** { **filter** | **ap** }

Syntax Description

source-priority	Enter the ap tag source priority. Valid range is 2 to 3.
source	Specifiy the source for which priority is been set.
filter	AP filter as tag source.
ap	AP as tag source.

Command Default

None

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Examples

The following example shows how to set AP as a tag source:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap tag-source-priority priority-value source ap
```

ap tag-sources revalidate

To revalidate the access point tag sources, use the **ap tag-sources revalidate** command.

ap tag-sources revalidate

Syntax Description

tag-sources	Tag Sources.
revalidate	Revalidate access point tag sources.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Examples

The following example shows how to revalidate the access point tag sources:

```
Device# ap tag-sources revalidate
```

ap vlan-tag

To configure VLAN tagging for all nonbridge APs, use the **ap vlan-tag** command.

ap vlan-tag *vlan-id*

Syntax Description

vlan-id	VLAN identifier.

Command Default

VLAN tagging is not enabled for nonbridge APs.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Example

The following example shows how to configure VLAN tagging for all non-bridge APs:

```
Device# ap vlan-tag 1000
```

assisted-roaming

To configure assisted roaming using 802.11k on a WLAN, use the **assisted-roaming** command. To disable assisted roaming, use the **no** form of this command.

assisted-roaming {**dual-list** | **neighbor-list** | **prediction**}

no assisted-roaming {**dual-list** | **neighbor-list** | **prediction**}

Syntax Description

dual-list	Configures a dual band 802.11k neighbor list for a WLAN. The default is the band that the client is currently associated with.
neighbor-list	Configures an 802.11k neighbor list for a WLAN.
prediction	Configures assisted roaming optimization prediction for a WLAN.

Command Default

Neighbor list and dual band support are enabled by default. The default is the band that the client is currently associated with.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

When you enable the assisted roaming prediction list, a warning appears and load balancing is disabled for the WLAN if load balancing is already enabled on the WLAN. To make changes to the WLAN, the WLAN must be in disabled state.

Example

The following example shows how to configure a 802.11k neighbor list on a WLAN:

```
Device(config-wlan)#assisted-roaming neighbor-list
```

The following example shows the warning message when load balancing is enabled on a WLAN. Load balancing must be disabled if it is already enabled when configuring assisted roaming:

```
Device(config)#wlan test-prediction 2 test-prediction
Device(config-wlan)#client vlan 43
Device(config-wlan)#no security wpa
Device(config-wlan)#load-balance
Device(config-wlan)#assisted-roaming prediction
WARNING: Enabling neighbor list prediction optimization may slow association and impact
VOICE client perform.
Are you sure you want to continue? (y/n)[y]: y
% Request aborted - Must first disable Load Balancing before enabling Assisted Roaming
Prediction Optimization on this WLAN.
```

avg-packet-size packetsize

To configure the wireless media-stream's average packet size, use the **avg-packet-size** command.

avg-packet-size *packetsize-value*

Syntax Description

packetsize-value	Average Packet Size. Valid range is 100 to 1500.

Command Default

None

Command Modes

media-stream

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Examples

The following example shows how to configure wireless media-stream's average packet size:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group doc-grp 224.0.0.0 224.0.0.223
Device(config-media-stream)# avg-packet-size500
```

band-select client

To configure the client threshold minimum dB for the selected band, use the **band-select client** command. To reset the client threshold minimum dB for the selected band, use the **no** form of this command.

band-select client { **mid-rssi** | **rssi** } *dBm value*

Syntax Description

mid-rssi	Minimum dBm of a client RSSI start to respond to probe
rssi	Minimum dBm of a client RSSI to respond to probe
dBm value	Minimum dBm of a client RSSI to respond to probe. Valid range is between –90 and –20 dBm.

Command Default

None

Command Modes

config-rf-profile

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

This command is enabled only for 2.4-GHz band.

This example shows how to set the client threshold to minimum dB for a selected band.

```
Device(config-rf-profile)#band-select client rssi -50
```

band-select cycle

To configure the band cycle parameters, use the **band-select cycle** command. To reset the threshold value, use the **no** form of this command.

band-select cycle { **count** | **threshold** } *value*

Syntax Description

count	Sets the Band Select probe cycle count.
value	Maximum number of cycles not responding. The range is between 1 and 10.
threshold	Sets the time threshold for a new scanning cycle.
value	Set the threshold value in milliseconds. The valid is between 1and 1000.

Command Default

None

Command Modes

config-rf-profile

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

None

This example shows how to configure the probe cycle count in an RF profile for a selected band.

```
Device(config-rf-profile)#band-select cycle count 5
```

band-select expire

To configure the expiry time for the RF profile for the selected band, use the **band-select expire** command. To reset the value, use the **no** form of this command.

band-select expire { **dual-band** | **suppression** } *value*
no band-select expire { **dual-band** | **suppression** }

Syntax Description

dual-band	Configures the RF Profile Band Select Expire Dual Band.
value	Setting the time to expire for pruning previously known dual-band clients. The range is between 10 and 300.
suppression	Configures the RF Profile Band Select Expire Suppression.
value	Setting the time to expire for pruning previously known 802.11b/g clients. The range is between 10 and 200.

Command Default

None

Command Modes

config-rf-profile

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

None

This example shows how to configure the time to expire for a dual-band of an RF profile in a selected band.

```
Device(config-rf-profile)#band-select expire dual-band 15
```

band-select probe-response

To configure the probe responses to the clients for a selected band, use the **band-select probe-response** command. To disable the probe-response, use the **no** form of this command.

band-select probe-response

Syntax Description

probe-response	Probe responses to clients.

Command Default

None

Command Modes

config-rf-profile

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

None

This example shows how to enable probe response to the clients.

```
Device(config-rf-profile)#band-select probe-response
```

bss-transition

To configure BSS transition per WLAN, use the **bss-transition** command.

bss-transition [**disassociation-imminent**]

Syntax Description

disassociation-imminent	BSS transition disassociation Imminent per WLAN.

Command Default

None

Command Modes

config-wlan

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Example

The following example shows how to configure BSS transition per WLAN:

```
Device(config-wlan)# bss-transition
```

call-snoop

call-snoop

no call-snoop

Syntax Description

This command has no keywords or arguments.

Command Default

VoIP snooping is disabled by default.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. The WLAN on which call snooping is configured must be configured with Platinum QoS. You must disable quality of service before using this command.

Example

This example shows how to enable VoIP on a WLAN:

```
Device# configure terminal
Device(config)# wireless profile policy policy-name
Device(config-wireless-policy)#service-policy input platinum-up
Device(config-wireless-policy)#service-policy output platinum
Device(config-wireless-policy)#call-snoop
Device(config-wireless-policy)#no shutdown
Device(config-wireless-policy)#end
```

captive-bypass-portal

To configure captive bypassing, use the **captive-bypass-portal** command.

captive-bypass-portal

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Example

This example shows how to configure captive bypassing for WLAN in LWA and CWA:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth WLAN1_MAP
Device(config)# captive-bypass-portal
Device(config)# wlan WLAN1_NAME 4 WLAN1_NAME
Device(config-wlan)# security web-auth
Device(config-wlan)# security web-auth parameter-map WLAN1_MAP
Device(config-wlan)# end
```

capwap-discovery

To set CAPWAP discovery response method as to whether a capwap-discovery response contains the public or private IP of the controller, use the **capwap-discovery** command.

capwap-discovery { **private** | **public** }

Syntax Description

private	Includes private IP in CAPWAP discovery response.
public	Includes public IP in CAPWAP discovery response.

Command Default

None

Command Modes

Management Interface Configuration(config-mgmt-interface)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

Example

The following example shows how to configure a CAPWAP discovery response method:

```
Device# configure terminal
Device(config)# wireless management interface Vlan1
Device(config-mgmt-interface)# capwap-discovery public
```

capwap backup

To configure a primary or secondary backup switch for all access points that are joined to a specific switch, use the **capwap backup** command.

capwap backup {**primary** *primary-controller-name primary-controller-ip-address* | **secondary** *secondary-controller-name secondary-controller-ip-address*}

Syntax Description

primary	Specifies the primary backup switch.
primary-controller-name	Primary backup switch name.
primary-controller-ip-address	Primary backup switch IP address.
secondary	Specifies the secondary backup switch.
secondary-controller-name	Secondary backup switch name.
secondary-controller-ip-address	Secondary backup switch IP address.

Command Default

None

Command Modes

AP profile configuration (config-ap-profile)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

This example shows how to configure a primary backup switch for all access points that are joined to a specific switch:

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# capwap backup primary controller1 192.0.2.51
```

This example shows how to configure a secondary backup switch for all access points that are joined to a specific switch:

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# capwap backup secondary controller1 192.0.2.52
```

cco-password (image-download-mode cco)

To configure the CCO server password for image dowload, use the **cco-password** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

`cco-password {0| 8}`<*Enter password*> <*Re-enter password*>

`no cco-password {0 | 8}`<*Enter password*> <*Re-enter password*>

Syntax Description

0	Specifies that an unencrypted password will follow.
8	Specifies that an AES encrypted password will follow.
password	Specifies the CCO server password.
re-enter password	Indicates that the user must re-enter the CCO server password.

Command Default

None

Command Modes

Wireless image download profile CCO configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode cco
Device(config-wireless-image-download-profile-cco)# cco-password 0 xxxxxxxx
```

cco-username (image-download-mode cco)

To configure the CCO username for image download, use the **cco-username**command. Use the **no** form of this command to negate the configuration or to set the command to its default.

`cco-username` *Username*

`no cco-username` *Username*

Syntax Description

username	Specifies the CCO username.

Command Default

None

Command Modes

Wireless image download profile CCO configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode cco
Device(config-wireless-image-download-profile-cco)# cco-username cco-server-username
```

cco-version (image-download-mode cco)

To configure and download the latest or the suggested version of the software image from CCO, use the **cco-version** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
cco-version {latest| suggested}

no cco-version {latest| suggested}
```

Syntax Description

latest	Configures and downloads the **latest** version of software image from CCO.
suggested	Configures and downloads the **suggested** version of software image from CCO. By default **suggested** version is selected.

Command Default

None

Command Modes

Wireless image download profile CCO configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode cco
Device(config-wireless-image-download-profile-cco)# cco-version suggested
```

cco-auto-check (image-download-mode cco)

To enable automatic check of the new software version on CCO, use the **cco-auto-check** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
cco-auto-check

no  cco-auto-check
```

Syntax Description

cco-auto-check	Enables the automatic check of the new software version at CCO every 30 days. This is applicable to Image Upgrade or Predownload only. By default the command is enabled.

Command Default

None

Command Modes

Wireless image download profile CCO configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode cco
Device(config-wireless-image-download-profile-cco)# cco-auto-check
```

ccx aironet-iesupport

To configure the support of Aironet IE CCX option, use the following command:

ccx aironet-iesupport

Syntax Description

ccx	Configures the Cisco Client Extension options.
aironet-iesupport	Sets the support of Aironet IE on WLAN.

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

Example

This example shows how to configure Aironet IE support:

```
Device(config-wlan)#ccx aironet-iesupport
```

cdp

To enable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point under the AP profile, use the **cdp** command. To disable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the **no** form of this command.

```
ap profile default-ap-profile

cdp
no  cdp
```

Command Default

Disabled on all access points.

Command Modes

AP profile mode (config-ap-profile)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

The **no cdp** command disables CDP on all access points that are joined to the switch and all access points that join in the future. CDP remains disabled on both current and future access points even after the switch or access point reboots. To enable CDP, enter the **cdp** command.

Note CDP over Ethernet/radio interfaces is available only when CDP is enabled. After you enable CDP on all access points joined to the switch, you can disable and then reenable CDP on individual access points using the **ap name** *Cisco-AP* **cdp** command. After you disable CDP on all access points joined to the switch, you can enable and then disable CDP on individual access points.

This example shows how to enable CDP on all access points:

```
Device(config)# ap profile default-ap-profile


Device(config-ap-profile)# cdp
```

central association

To enable central association for locally switched clients, use the **central association** command.

central association

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Example

The following example shows how to enable enable central association for locally switched clients:

```
Device(config-wireless-policy)# central association
```

central authentication

To enable or disable central authentication, use the **central authentication** command.

central authentication

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Example

The following example shows how to enable central authentication:

```
Device(config-wireless-policy)# central authentication
```

central dhcp

To enable central dhcp for locally switched clients, use the **central dhcp** command.

central dhcp

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to enable central dhcp for locally switched clients:

```
Device(config-wireless-policy)# central dhcp
```

central-webauth

To configure central-webauth for an ACL, use the **central-webauth** command.

central-webauth

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to configure central-webauth for an ACL:

```
Device(config-wireless-policy)# central-webauth
```

chassis redundancy keep-alive

To configure peer keep-alive retries and time interval before claiming peer is down, use the **chassis redundancy keep-alive** command.

chassis redundancy keep-alive { **retries** *retries* | **timer** *timer* }

Syntax Description

retries	Chassis peer keep-alive retries before claiming peer is down. Valid values range from 5 to 10, enter 5 for default.
timer	Chassis peer keep-alive time interval in multiple of 100 ms. Valid values range from 1 to 10, enter 1 for default.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure peer keep-alive retries and time interval:

```
Device# chassis redundancy keep-alive retries 6
Device# chassis redundancy keep-alive timer 6
```

chassis renumber

To renumber the local chassis id assignment, use the **chassis renumber** command.

chassis *chassis-num* **renumber** *renumber-id*

Syntax Description

chassis-num	Chassis number.
renumber-id	Local chassis id.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to renumber the local chassis id assignment:

```
Device# chassis 1 renumber 1
```

chassis transport

To enable or disable chassis transport, use the **chassis transport** command.

chassis *chassis-num* **transport** {**enable** | **disable**}

Syntax Description

chassis-num	Chassis number.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to enable chassis transport:

```
Device# chassis 1 transport enable
```

class

To define a traffic classification match criteria for the specified class-map name, use the **class** command in policy-map configuration mode. Use the **no** form of this command to delete an existing class map.

class {*class-map-name* | **class-default**}
no class {*class-map-name* | **class-default**}

Syntax Description

class-map-name	The class map name.
class-default	Refers to a system default class that matches unclassified packets.

Command Default

No policy map class-maps are defined.

Command Modes

Policy-map configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

Before using the **class** command, you must use the **policy-map** global configuration command to identify the policy map and enter policy-map configuration mode. After specifying a policy map, you can configure a policy for new classes or modify a policy for any existing classes in that policy map. You attach the policy map to a port by using the **service-policy** interface configuration command.

After entering the **class** command, you enter the policy-map class configuration mode. These configuration commands are available:

- **exit**—Exits the policy-map class configuration mode and returns to policy-map configuration mode.
- **no**—Returns a command to its default setting.
- **police**—Defines a policer or aggregate policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information about this command, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com.
- **set**—Specifies a value to be assigned to the classified traffic. For more information, see set, on page 425

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

The **class** command performs the same function as the **class-map** global configuration command. Use the **class** command when a new classification, which is not shared with any other ports, is needed. Use the **class-map** command when the map is shared among many ports.

You can configure a default 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 default traffic.

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Examples

This example shows how to create a policy map called policy1. When attached to the ingress direction, it matches all the incoming traffic defined in class1, sets the IP Differentiated Services Code Point (DSCP) to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic exceeding the profile is marked down to a DSCP value gotten from the policed-DSCP map and then sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action
Device(config-pmap-c)# police 1000000 20000 exceed-action
Device(config-pmap-c)# exit
```

This example shows how to configure a default traffic class to a policy map. It also shows how the default traffic class is automatically placed at the end of policy-map pm3 even though **class-default** was configured first:

```
Device# configure terminal
Device(config)# class-map cm-3
Device(config-cmap)# match ip dscp 30
Device(config-cmap)# exit

Device(config)# class-map cm-4
Device(config-cmap)# match ip dscp 40
Device(config-cmap)# exit

Device(config)# policy-map pm3
Device(config-pmap)# class class-default
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-3
Device(config-pmap-c)# set dscp 4
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-4
Device(config-pmap-c)# set precedence 5
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device# show policy-map pm3
Policy Map pm3
  Class cm-3
    set dscp 4
  Class cm-4
    set precedence 5
  Class class-default
    set dscp af11
```

classify

To classify a rule for rogue devices, use the **classify** command.

classify {**friendly** | **malicious** | **delete**}

Syntax Description

friendly	Classifies devices matching this rule as friendly.
malicious	Classifies devices matching this rule as malicious.
delete	Devices matching this rule are ignored.

Command Default

None

Command Modes

config-rule

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to classify rogue devices as friendly:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless wps rogue rule my-rogue-rule priority 3
Device(config-rule)# classify friendly
```

class-map

To create a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode, use the **class-map** command in global configuration mode. Use the **no** form of this command to delete an existing class map and to return to global or policy map configuration mode.

class-map [{**match-any***type*}][{**match-all***type*}] *class-map-name*
no class-map [{**match-any***type*}][{**match-all***type*}] *class-map-name*

Syntax Description

match-any	(Optional) Performs a logical-OR of the matching statements under this class map. One or more criteria must be matched.
match-all	(Optional) Performs a logical-AND all matching statements under this classmap.
type	(Optional) Configures the CPL class map.
class-map-name	The class map name.

Command Default

No class maps are defined.

Command Modes

Global configuration

Policy map configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode.

The **class-map** command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-port basis.

After you are in quality of service (QoS) class-map configuration mode, these configuration commands are available:

- **description**—Describes the class map (up to 200 characters). The **show class-map** privileged EXEC command displays the description and the name of the class map.
- **exit**—Exits from QoS class-map configuration mode.
- **match**—Configures classification criteria.
- **no**—Removes a match statement from a class map.

If you enter the **match-any** keyword, you can only use it to specify an extended named access control list (ACL) with the **match access-group** class-map configuration command.

To define packet classification on a physical-port basis, only one **match** command per class map is supported.

The ACL can have multiple access control entries (ACEs).

Examples

This example shows how to configure the class map called class1 with one match criterion, which is an access list called 103:

```
Device(config)# access-list 103 permit ip any any dscp 10
Device(config)# class-map class1
Device(config-cmap)# match access-group 103
Device(config-cmap)# exit
```

This example shows how to delete the class map class1:

```
Device(config)# no class-map class1
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

clear chassis redundancy

To clear high-availability (HA) configuration, use the **clear chassis redundancy** command.

clear chassis redundancy

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to clear HA configuration:

```
Device# clear chassis redundancy
```

clear mdns-sd statistics

To clear mDNS statistics, use the **clear mdns-sd statistics** command.

clear mdns-sd statistics { **debug** | **glan-id** *<1 - 5>* | **rlan-id** *<1 - 128>* **wired** | **wlan-id** *<1 - 4096>* }

Syntax Description

debug	Clears the mDNS debug statistics.
glan-id*<1 - 5>*	Clears the GLAN ID. The value range is from 1 to 5.
rlan-id*<1 - 128>*	Clears the RLAN ID. The value range is from 1 to 128.
wired	Clears the mDNS wired statistics.
wlan-id*<1 - 4096>*	Clears the WLAN ID. The value range is from 1 to 4096.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to clear the mDNS statistics:

```
Device# clear mdns-sd statistics
```

clear platform condition all

To clear all conditional debug and packet-trace configuration and data, use the **clear platform condition all** command.

clear platform condition all

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to clear all conditional debug and packet-trace configuration and data:

```
Device# clear platform condition all
```

clear wireless wps rogue ap

To clear all rogue APs or rogue APs with specific MAC addresses, use the **clear wireless wps rogue ap** command.

clear wireless wps rogue ap { **all** | **mac-address** <*MAC Address*> }

Syntax Description

all	Clears all the rogue APs.
mac-address <*MAC Address*>	Clears the rogue APs with specific MAC addresses.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to clear all rogue APs or rogue APs with specific MAC addresses:

```
Device# clear wireless wps rogue ap all
Device# clear wireless wps rogue ap mac-address 10.10.1
```

clear wireless wps rogue client

To clear all rogue clients or client with specific MAC addresses, use the **clear wireless wps rogue client** command.

clear wireless wps rogue client { **all** | **mac-address** <*MAC Address*> }

Syntax Description

all	Clears all the rogue clients.
mac-address <*MAC Address*>	Clears the rogue clients with specific MAC addresses.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to clear all rogue clients or rogue clients with specific MAC addresses:

```
Device# clear wireless wps rogue client all
Device# clear wireless wps rogue client mac-address 10.10.1
```

clear wireless wps rogue stats

To clear rogue statistics, use the **clear wireless wps rogue stats** command.

clear wireless wps rogue stats

Syntax Description

This command has no arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to clear rogue statistics:

```
Device# clear wireless wps rogue stats
```

client association limit

To configure the maximum number of client connections on a WLAN, use the **client association limit** command. To disable clients association limit on the WLAN, use the **no** form of this command.

client association limit {*association-limit*}
no client association limit {*association-limit*}

Syntax Description

association-limit	Number of client connections to be accepted. The range is from 0 to . A value of zero (0) indicates no set limit.

Command Default

The maximum number of client connections is set to 0 (no limit).

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to configure a client association limit on a WLAN and configure the client limit to 200:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# client association limit 200
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to disable a client association limit on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# no client association limit
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to configure a client association limit per radio on a WLAN and configure the client limit to 200:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client association limit radio 200
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to configure a client association limit per AP on a WLAN and configure the client limit to 300::

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client association limit ap 300
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

channel foreign

To configure the RF Profile DCA foreign AP contribution, use the **channel foreign** command. To disable the DCA Foreign AP Contribution, use the **no** form of this command.

channel foreign

Syntax Description

foreign	Configures the RF Profile DCA foreign AP contribution.

Command Default

None

Command Modes

config-rf-profile

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

None

This example shows how to configure the RF profile DCA foreign AP contribution.

```
Device(config-rf-profile)#channel foreign
```

client-l2-vnid

To configure the client l2-vnid on a wireless fabric profile, use the **client-l2-vnid** command.

client-l2-vnid *vnid*

Syntax Description

vnid	Configures client l2-vnid. Valid range is 0 to 16777215.

Command Default

None

Command Modes

config-wireless-fabric

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the client l2-vnid value on a wireless fabirc profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile fabric fabric-profile-name
Device(config-wireless-fabric)# client-l2-vnid 10
```

convergence

To configure mesh convergence method, use the **convergence** command.

convergence { **fast** | **noise-tolerant-fast** | **standard** | **very-fast** }

Syntax Description

fast	Configures fast convergence method.
noise-tolerant-fast	Configures noise-tolerant fast convergence method method to handle unstable RF environment.
standard	Configures standard convergence method.
very-fast	Configures very fast convergence method.

Command Default

Standard

Command Modes

config-wireless-mesh-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the fast convergence method for a mesh AP profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile mesh mesh-profile
Device(config-wireless-mesh-profile)# convergence fast
```

coverage

To configure the voice and data coverage, use the **coverage** command. To reset the minimum RSSI value use the **no** form of this command.

coverage {**data** | **voice**} **rssi threshold** *value*

Syntax Description

data	Configure Coverage Hole Detection for data packets.
voice	Configure Coverage Hole Detection for voice packets.
value	Minimum RSSI value for the packets received by the access point. The valid rage is between –90 and –60 dBm.

Command Default

None

Command Modes

config-rf-profile

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

None

This example shows how to configure the coverage hole detection for data packets.

```
Device(config-rf-profile)#coverage data rssi threshold –85
```

crypto key generate rsa

To generate Rivest, Shamir, and Adelman (RSA) key pairs, use the **crypto key generate rsa** commandinglobal configuration mode.

crypto key generate rsa [{**general-keys** | **usage-keys** | **signature** | **encryption**}] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename* **:**] [**redundancy**] [**on** *devicename* **:**]

Syntax Description

general-keys	(Optional) Specifies that a general-purpose key pair will be generated, which is the default.
usage-keys	(Optional) Specifies that two RSA special-usage key pairs, one encryption pair and one signature pair, will be generated.
signature	(Optional) Specifies that the RSA public key generated will be a signature special usage key.
encryption	(Optional) Specifies that the RSA public key generated will be an encryption special usage key.
label *key-label*	(Optional) Specifies the name that is used for an RSA key pair when they are being exported. If a key label is not specified, the fully qualified domain name (FQDN) of the router is used.
exportable	(Optional) Specifies that the RSA key pair can be exported to another Cisco device, such as a router.
modulus *modulus-size*	(Optional) Specifies the IP size of the key modulus. By default, the modulus of a certification authority (CA) key is 1024 bits. The recommended modulus for a CA key is 2048 bits. The range of a CA key modulus is from 350 to 4096 bits. **Note** Effective with Cisco IOS XE Release 2.4 and Cisco IOS Release 15.1(1)T, the maximum key size was expanded to 4096 bits for private key operations. The maximum for private key operations prior to these releases was 2048 bits.
storage *devicename* **:**	(Optional) Specifies the key storage location. The name of the storage device is followed by a colon (:).
redundancy	(Optional) Specifies that the key should be synchronized to the standby CA.
on *devicename* **:**	(Optional) Specifies that the RSA key pair will be created on the specified device, including a Universal Serial Bus (USB) token, local disk, or NVRAM. The name of the device is followed by a colon (:). Keys created on a USB token must be 2048 bits or less.

Command Default

RSA key pairs do not exist.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(8)T	The *key-label* argumentwas added.
12.2(15)T	The **exportable** keyword was added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The **storage** keyword and *devicename* **:** argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **storage** keyword and *devicename* **:** argument were implemented on the Cisco 7200VXR NPE-G2 platform. The **signature**, **encryption** and **on** keywords and *devicename* **:** argument were added.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.
XE 2.4	The maximum RSA key size was expanded from 2048 to 4096 bits for private key operations.
15.0(1)M	This command was modified. The **redundancy** keyword was introduced.
15.1(1)T	This command was modified. The range value for the **modulus** keyword value is extended from 360 to 2048 bits to 360 to 4096 bits.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Use this command to generate RSA key pairs for your Cisco device (such as a router).

RSA keys are generated in pairs--one public RSA key and one private RSA key.

If your router already has RSA keys when you issue this command, you will be warned and prompted to replace the existing keys with new keys.

Note Before issuing this command, ensure that your router has a hostname and IP domain name configured (with the **hostname** and **ip domain-name** commands). You will be unable to complete the **crypto key generate rsa** command without a hostname and IP domain name. (This situation is not true when you generate only a named key pair.)

Note Secure Shell (SSH) may generate an additional RSA key pair if you generate a key pair on a router having no RSA keys. The additional key pair is used only by SSH and will have a name such as {*router_FQDN* }.server. For example, if a router name is "router1.cisco.com," the key name is "router1.cisco.com.server."

This command is not saved in the router configuration; however, the RSA keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.

Note If the configuration is not saved to NVRAM, the generated keys are lost on the next reload of the router.

There are two mutually exclusive types of RSA key pairs: special-usage keys and general-purpose keys. When you generate RSA key pairs, you will be prompted to select either special-usage keys or general-purpose keys.

Special-Usage Keys

If you generate special-usage keys, two pairs of RSA keys will be generated. One pair will be used with any Internet Key Exchange (IKE) policy that specifies RSA signatures as the authentication method, and the other pair will be used with any IKE policy that specifies RSA encrypted keys as the authentication method.

A CA is used only with IKE policies specifying RSA signatures, not with IKE policies specifying RSA-encrypted nonces. (However, you could specify more than one IKE policy and have RSA signatures specified in one policy and RSA-encrypted nonces in another policy.)

If you plan to have both types of RSA authentication methods in your IKE policies, you may prefer to generate special-usage keys. With special-usage keys, each key is not unnecessarily exposed. (Without special-usage keys, one key is used for both authentication methods, increasing the exposure of that key.)

General-Purpose Keys

If you generate general-purpose keys, only one pair of RSA keys will be generated. This pair will be used with IKE policies specifying either RSA signatures or RSA encrypted keys. Therefore, a general-purpose key pair might get used more frequently than a special-usage key pair.

Named Key Pairs

If you generate a named key pair using the *key-label*argument, you must also specify the **usage-keys** keyword or the **general-keys** keyword. Named key pairs allow you to have multiple RSA key pairs, enabling the Cisco IOS software to maintain a different key pair for each identity certificate.

Modulus Length

When you generate RSA keys, you will be prompted to enter a modulus length. The longer the modulus, the stronger the security. However a longer modules takes longer to generate (see the table below for sample times) and takes longer to use.

Table 7: Sample Times by Modulus Length to Generate RSA Keys

Router	360 bits	512 bits	1024 bits	2048 bits (maximum)
Cisco 2500	11 seconds	20 seconds	4 minutes, 38 seconds	More than 1 hour
Cisco 4700	Less than 1 second	1 second	4 seconds	50 seconds

Cisco IOS software does not support a modulus greater than 4096 bits. A length of less than 512 bits is normally not recommended. In certain situations, the shorter modulus may not function properly with IKE, so we recommend using a minimum modulus of 2048 bits.

Note As of Cisco IOS Release 12.4(11)T, peer *public* RSA key modulus values up to 4096 bits are automatically supported. The largest private RSA key modulus is 4096 bits. Therefore, the largest RSA private key a router may generate or import is 4096 bits. However, RFC 2409 restricts the private key size to 2048 bits or less for RSA encryption. The recommended modulus for a CA is 2048 bits; the recommended modulus for a client is 2048 bits.

Additional limitations may apply when RSA keys are generated by cryptographic hardware. For example, when RSA keys are generated by the Cisco VPN Services Port Adapter (VSPA), the RSA key modulus must be a minimum of 384 bits and must be a multiple of 64.

Specifying a Storage Location for RSA Keys

When you issue the **crypto key generate rsa** command with the **storage** *devicename* **:** keyword and argument, the RSA keys will be stored on the specified device. This location will supersede any **crypto key storage** command settings.

Specifying a Device for RSA Key Generation

As of Cisco IOS Release 12.4(11)T and later releases, you may specify the device where RSA keys are generated. Devices supported include NVRAM, local disks, and USB tokens. If your router has a USB token configured and available, the USB token can be used as cryptographic device in addition to a storage device. Using a USB token as a cryptographic device allows RSA operations such as key generation, signing, and authentication of credentials to be performed on the token. The private key never leaves the USB token and is not exportable. The public key is exportable.

RSA keys may be generated on a configured and available USB token, by the use of the **on** *devicename* **:** keyword and argument. Keys that reside on a USB token are saved to persistent token storage when they are generated. The number of keys that can be generated on a USB token is limited by the space available. If you attempt to generate keys on a USB token and it is full you will receive the following message:

```
% Error in generating keys:no available resources
```

Key deletion will remove the keys stored on the token from persistent storage immediately. (Keys that do not reside on a token are saved to or deleted from nontoken storage locations when the **copy**or similar command is issued.)

For information on configuring a USB token, see " Storing PKI Credentials " chapter in the Cisco IOS Security Configuration Guide, Release 12.4T. For information on using on-token RSA credentials, see the " Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment " chapter in the Cisco IOS Security Configuration Guide , Release 12.4T.

Specifying RSA Key Redundancy Generation on a Device

You can specify redundancy for existing keys only if they are exportable.

Examples

The following example generates a general-usage 1024-bit RSA key pair on a USB token with the label "ms2" with crypto engine debugging messages shown:

```
Router(config)# crypto key generate rsa label ms2 modulus 2048 on usbtoken0:
```

```
The name for the keys will be: ms2
% The key modulus size is 2048 bits
% Generating 1024 bit RSA keys, keys will be on-token, non-exportable...
Jan 7 02:41:40.895: crypto_engine: Generate public/private keypair [OK]
Jan 7 02:44:09.623: crypto_engine: Create signature
Jan 7 02:44:10.467: crypto_engine: Verify signature
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_CREATE_PUBKEY(hw)(ipsec)
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_PUB_DECRYPT(hw)(ipsec)
```

Now, the on-token keys labeled “ms2” may be used for enrollment.

The following example generates special-usage RSA keys:

```
Router(config)# crypto key generate rsa usage-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

The following example generates general-purpose RSA keys:

Note You cannot generate both special-usage and general-purpose keys; you can generate only one or the other.

```
Router(config)# crypto key generate rsa general-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

The following example generates the general-purpose RSA key pair “exampleCAkeys”:

```
crypto key generate rsa general-keys label exampleCAkeys
crypto ca trustpoint exampleCAkeys
 enroll url
http://exampleCAkeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

The following example specifies the RSA key storage location of “usbtoken0:” for “tokenkey1”:

crypto key generate rsa general-keys label tokenkey1 storage usbtoken0:

The following example specifies the **redundancy** keyword:

```
Router(config)# crypto key generate rsa label MYKEYS redundancy
```

The name for the keys will be: MYKEYS

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]:

% Generating 512 bit RSA keys, keys will be non-exportable with redundancy...[OK]

Related Commands

Command	Description
copy	Copies any file from a source to a destination, use the copy command in privileged EXEC mode.
crypto key storage	Sets the default storage location for RSA key pairs.
debug crypto engine	Displays debug messages about crypto engines.
hostname	Specifies or modifies the hostname for the network server.
ip domain-name	Defines a default domain name to complete unqualified hostnames (names without a dotted-decimal domain name).
show crypto key mypubkey rsa	Displays the RSA public keys of your router.
show crypto pki certificates	Displays information about your PKI certificate, certification authority, and any registration authority certificates.

cts inline-tagging

To configure Cisco TrustSec (CTS) inline tagging, use the **cts inline-tagging** command.

cts inline-tagging

Syntax Description

This command has no keywords or arguments.

Command Default

Inline tagging is not configured.

Command Modes

wireless policy configuration (config-wireless-policy)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to configure CTS inline tagging.

```
Device(config-wireless-policy)# cts inline-tagging
```

cts role-based enforcement

To configure Cisco TrustSec (CTS) SGACL enforcement, use the **cts role-based enforcement** command.

cts role-based enforcement

Syntax Description

This command has no keywords or arguments.

Command Default

SGACL is not enforced.

Command Modes

wireless policy configuration (config-wireless-policy)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to configure CTS SGACL enforcement.

```
Device(config-wireless-policy)# cts role-based enforcement
```

cts sgt

To set the Cisco TrustSec (CTS) default security group tag (SGT), use the **cts sgt** command.

cts sgt *sgt-value*

Syntax Description

sgt-value	Security group tag value.

Command Default

SGT tag is not set.

Command Modes

wireless policy configuration (config-wireless-policy)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to set the default SGT.

```
Device(config-wireless-policy)# cts sgt 100
```

custom-page login device

To configure a customized login page, use the **custom-page login device** command.

custom-page login device *html-filename*

Syntax Description

html-filename	Enter the HTML filename of the login page.

Command Default

None

Command Modes

config-params-parameter-map

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure a customized login page:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-map-name
Device(config-params-parameter-map)# custom-page login device bootflash:login.html
```

default

To set the parameters to their default values, use the **default** command.

default {**aaa-override** | **accounting-list** | **band-select** | **broadcast-ssid** | **call-snoop** | **ccx** | **channel-scan** | **parameters** | **chd** | **client** | **datalink** | **diag-channel** | **dtim** | **exclusionlist** | **ip** | **ipv6** | **load-balance** | **local-auth** | **mac-filtering** | **media-stream** | **mfp** | **mobility** | **nac** | **passive-client** | **peer-blocking** | **radio** | **roamed-voice-client** | **security** | **service-policy** | **session-timeout** | **shutdown** | **sip-cac** | **static-ip** | **uapsd** | **wgb** | **wmm**}

Syntax Description

aaa-override	Sets the AAA override parameter to its default value.
accounting-list	Sets the accounting parameter and its attributes to their default values.
band-select	Sets the band selection parameter to its default values.
broadcast-ssid	Sets the broadcast Service Set Identifier (SSID) parameter to its default value.
call-snoop	Sets the call snoop parameter to its default value.
ccx	Sets the Cisco client extension (Cisco Aironet IE) parameters and attributes to their default values.
channel-scan	Sets the channel scan parameters and attributes to their default values.
chd	Sets the coverage hold detection parameter to its default value.
client	Sets the client parameters and attributes to their default values.
datalink	Sets the datalink parameters and attributes to their default values.
diag-channel	Sets the diagnostic channel parameters and attributes to their default values.
dtim	Sets the Delivery Traffic Indicator Message (DTIM) parameter to its default value.
exclusionlist	Sets the client exclusion timeout parameter to its default value.
ip	Sets the IP parameters to their default values.
ipv6	Sets the IPv6 parameters and attributes to their default values.
load-balance	Sets the load-balancing parameter to its default value.
local-auth	Sets the Extensible Authentication Protocol (EAP) profile parameters and attributes to their default values.
mac-filtering	Sets the MAC filtering parameters and attributes to their default values.
media-stream	Sets the media stream parameters and attributes to their default values.

mfp	Sets the Management Frame Protection (MPF) parameters and attributes to their default values.
mobility	Sets the mobility parameters and attributes to their default values.
nac	Sets the RADIUS Network Admission Control (NAC) parameter to its default value.
passive-client	Sets the passive client parameter to its default value.
peer-blocking	Sets the peer to peer blocking parameters and attributes to their default values.
radio	Sets the radio policy parameters and attributes to their default values.
roamed-voice-client	Sets the roamed voice client parameters and attributes to their default values.
security	Sets the security policy parameters and attributes to their default values.
service-policy	Sets the WLAN quality of service (QoS) policy parameters and attributes to their default values.
session-timeout	Sets the client session timeout parameter to its default value.
shutdown	Sets the shutdown parameter to its default value.
sip-cac	Sets the Session Initiation Protocol (SIP) Call Admission Control (CAC) parameters and attributes to their default values.
static-ip	Sets the static IP client tunneling parameters and their attributes to their default values.
uapsd	Sets the Wi-Fi Multimedia (WMM) Unscheduled Automatic Power Save Delivery (UAPSD) parameters and attributes to their default values.
wgb	Sets the Workgroup Bridges (WGB) parameter to its default value.
wmm	Sets the WMM parameters and attributes to their default values.

Command Default

None.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to set the Cisco Client Extension parameter to its default value:

```
Device(config-wlan)# default ccx aironet-iesupport
```

description

To configure a description for a flow monitor, flow exporter, or flow record, use the **description** command in the appropriate configuration mode. To remove a description, use the **no** form of this command.

description *description*
no description *description*

Syntax Description

description	Text string that describes the flow monitor, flow exporter, or flow record.

Command Default

The default description for a flow sampler, flow monitor, flow exporter, or flow record is "User defined."

Command Modes

The following command modes are supported:

Flow exporter configuration

Flow monitor configuration

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

To return this command to its default setting, use the **no description** or **default description** command in the appropriate configuration mode.

The following example configures a description for a flow monitor:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# description Monitors traffic to 172.16.0.1 255.255.0.0
```

destination

To configure an export destination for a flow exporter, use the **destination** command in flow exporter configuration mode. To remove an export destination for a flow exporter, use the **no** form of this command.

destination {*hostnameip-address*}
no destination {*hostnameip-address*}

Syntax Description

hostname	Hostname of the device to which you want to send the NetFlow information.
ip-address	IPv4 address of the workstation to which you want to send the NetFlow information.

Command Default

An export destination is not configured.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

Each flow exporter can have only one destination address or hostname.

When you configure a hostname instead of the IP address for the device, the hostname is resolved immediately and the IPv4 address is stored in the running configuration. If the hostname-to-IP-address mapping that was used for the original Domain Name System (DNS) name resolution changes dynamically on the DNS server, the switch does not detect this, and the exported data continues to be sent to the original IP address, resulting in a loss of data.

To return this command to its default setting, use the **no destination** or **default destination** command in flow exporter configuration mode.

The following example shows how to configure the networking device to export the cache entry to a destination system:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# destination 10.0.0.4
```

device-tracking binding vlan

To configure IPv4 or IPv6 static entry, use the **device-tracking binding vlan** command.

device-tracking binding vlan *vlan-id* {*ipv4-addr ipv6-addr* }**interface gigabitEthernet** *ge-intf-num hardware-or-mac-address*

Syntax Description

vlan-id	VLAN ID. Valid range is 1 to 4096.
ipv4-addr	IPv4 address of the device.
interface gigabitEthernet	GigabitEthernet IEEE 802.3z.
ge-intf-num	GigabitEthernet interface number. Valid range is 1 to 32.
hardware-or-mac-address	The 48-bit hardware address or the MAC address of the device.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure IPv4 static entry:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# device-tracking binding vlan 20 20.20.20.5 interface gigabitEthernet 1
0000.1111.2222
```

dhcp-tlv-caching

To configure DHCP TLV caching on a WLAN, use the **dhcp-tlv-caching** command.

dhcp-tlv-caching

Command Default None

Command Modes config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to configure DHCP TLV caching on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy rr-xyz-policy-1
Device(config-wireless-policy)# dhcp-tlv-caching
Device(config-wireless-policy)# radius-profiling
Device(config-wireless-policy)# end
```

dnscrypt

To enable or disable DNScrypt, use the **dnscrypt** command.

dnscrypt

Command Default

None

Command Modes

config-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

By default, the DNScrypt option is enabled.

This example shows how to enable or disable DNScrypt:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type umbrella global
Device(config-profile)# token 57CC80106C087FB1B2A7BAB4F2F4373C00247166
Device(config-profile)# local-domain dns_wl
Device(config-profile)# no dnscrypt
Device(config-profile)# end
```

domain-name (DHCP)

To specify the domain n ame for a Dynamic Host Configuration Protocol (DHCP) client, use the **domain-name** command in DHCP pool configuration mode. To remove the domain name, use the no form of this command.

domain-name *domain*
no domain-name

Syntax Description

domain	Specifies the domain name string of the client.

Command Default

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies cisco.com as the domain name of the client:

```
domain-name cisco.com
```

Related Commands

Command	Description
dns-server	Specifies the DNS IP servers available to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

dot11ax twt-broadcast-support

To configure TWT broadcast support on WLAN, use the **dot11ax twt-broadcast-support** command. To disable the feature, use the **no** command of the command.

dot11ax twt-broadcast-support

[no] dot11ax twt-broadcast-support

Syntax Description

dot11ax twt-broadcast-support	Configures the TWT broadcast support on WLAN

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

Example

This example shows how to configure target wakeup time on WLAN:

```
Device(config-wlan)# dot11ax twt-broadcast-support
```

dot11 5ghz reporting-interval

To configure the client report interval sent from AP for clients on 802.11a radio, use the **dot11 5ghz reporting-interval** command.

dot11 5ghz reporting-interval *reporting-interval*

Syntax Description

reporting-interval	Interval at which client report needs to be sent in seconds.

Command Default

None

Command Modes

config-ap-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to set the client report interval in seconds:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap profile profile-name
Device(config-ap-profile)# dot11 5ghz reporting-interval 8
```

dot11 reporting-interval

To set the volume metering interval, use the **dot11 reporting-interval** command.

dot11 { **24ghz** | **5ghz** } *reporting-interval*

Syntax Description

reporting-interval	Interval to send client accounting statistics.

Command Default

Interval is configured at the default level of 90 seconds.

Command Modes

config-ap-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Though the CLI allows you to configure range from 5 to 90 seconds, we recommend that you use 60 to 90 seconds range for Volume Metering.

This CLI can also be used to configure the interval when smart roam is enabled, which has a range of 5 to 90 seconds.

Though you can set two different values for volume metering and smart roam, only one value takes effect based on the order of execution. So, we recommend that you use the same reporting interval for both.

Example

The following example shows how to configure volume metering:

```
Device(config-ap-profile)# dot11 24ghz 60
```

dot1x system-auth-control

To globally enable 802.1X SystemAuthControl (port-based authentication), use the **dot1x system-auth-control**command in global configuration mode. To disable SystemAuthControl, use the **no** form of this command.

dot1x system-auth-control
no dot1x system-auth-control

Syntax Description

This command has no arguments or keywords.

Command Default

System authentication is disabled by default. If this command is disabled, all ports behave as if they are force authorized.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

The **no** form of the command removes any 802.1X-related configurations.

You must enable Authentication, Authorization, and Accounting (AAA) and specify the authentication method list before enabling 802.1X. A method list describes the sequence and authentication methods to be queried to authenticate a user.

Examples

The following example shows how to enable SystemAuthControl:

```
Router(config)# dot1x system-auth-control
```

Related Commands

Command	Description
aaa authentication dot1x	Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.
aaa new-model	Enables the AAA access-control model.
debug dot1x	Displays 802.1X debugging information.
description	Specifies a description for an 802.1X profile.
device	Statically authorizes or rejects individual devices.
dot1x initialize	Initializes 802.1X state machines on all 802.1X-enabled interfaces.
dot1x max-req	Sets the maximum number of times that a router or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
dot1x port-control	Enables manual control of the authorized state of a controlled port.
dot1x re-authenticate	Manually initiates a reauthentication of the specified 802.1X-enabled ports.
dot1x reauthentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
dot1x timeout	Sets retry timeouts.
identity profile	Creates an identity profile and enters identity profile configuration mode.
show dot1x	Displays details and statistics for an identity profile.
template	Specifies a virtual template from which commands may be cloned.

eap profile

To configure an EAP profile, use the **eap profile** command.

eap profile *profile-name*

Syntax Description

profile-name	Name of the EAP profile. Maximum number of allowed characters is 63.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure an EAP profile name:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# eap profile eap-profile-name
```

exclusionlist

To configure an exclusion list on a wireless LAN, use the **exclusionlist** command. To disable an exclusion list, use the **no** form of this command.

exclusionlist [**timeout** *seconds*]
no exclusionlist [**timeout**]

Syntax Description

timeout *seconds*	(Optional) Specifies an exclusion list timeout in seconds. The range is from 0 to 2147483647. A value of zero (0) specifies no timeout.

Command Default

The exclusion list is set to 60 seconds.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to configure a client exclusion list for a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# exclusionlist timeout 345
```

This example shows how to disable a client exclusion list on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no exclusionlist timeout 345
```

exporter default-flow-exporter

To add an exporter to use to export records, use the **exporter default-flow-exporter** command. Use the **no** form of this command to disable the feature.

exporter default-flow-exporter

[no] exporter default-flow-exporter

Syntax Description

There are no arguments to this command.

Command Default

None

Command Modes

Flow monitor configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

Example

This example shows how to add an exporter to use to export records:

```
Device(config-flow-monitor)#exporter default-flow-exporter
```

fallback-radio-shut

To configure shutdown of the radio interface, use the **fallback-radio-shut** command.

fallback-radio-shut

Command Default None

Command Modes config-wireless-flex-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure shutdown of the radio interface:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile flex flex-profile-name
Device(config-wireless-flex-profile)# fallback-radio-shut
```

flex

To configure flex related parameters, use the **flex** command.

flex {**nat-pat** | **split-mac-acl** *split-mac-acl-name* | **vlan-central-switching** }

Syntax Description

nat-pat	Enables NAT-PAT.
split-mac-acl	Configures split-mac-acl name.
split-mac-acl-name	Name of split MAC ACL.
vlan-central-switching	VLAN based central switching.

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure flex related VLAN central-switching:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy profile-name
Device(config-wireless-policy)# flex vlan-central-switching
```

flow exporter

To create a flow exporter, or to modify an existing flow exporter, and enter flow exporter configuration mode, use the **flow exporter** command in global configuration mode. To remove a flow exporter, use the **no** form of this command.

flow exporter *exporter-name*
no flow exporter *exporter-name*

Syntax Description

exporter-name	Name of the flow exporter that is being created or modified.

Command Default

flow exporters are not present in the configuration.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector, for analysis and storage. Flow exporters are created as separate entities in the configuration. Flow exporters are assigned to flow monitors to provide data export capability for the flow monitors. You can create several flow exporters and assign them to one or more flow monitors to provide several export destinations. You can create one flow exporter and apply it to several flow monitors.

Examples

The following example creates a flow exporter named FLOW-EXPORTER-1 and enters flow exporter configuration mode:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)#
```

flow monitor

To create a flow monitor, or to modify an existing flow monitor, and enter flow monitor configuration mode, use the **flow monitor** command in global configuration mode. To remove a flow monitor, use the **no** form of this command.

flow monitor *monitor-name*
no flow monitor *monitor-name*

Syntax Description

monitor-name	Name of the flow monitor that is being created or modified.

Command Default

flow monitors are not present in the configuration.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

Flow monitors are the component that is applied to interfaces to perform network traffic monitoring. Flow monitors consist of a flow record and a cache. You add the record to the flow monitor after you create the flow monitor. The flow monitor cache is automatically created at the time the flow monitor is applied to the first interface. Flow data is collected from the network traffic during the monitoring process based on the key and nonkey fields in the flow monitor's record and stored in the flow monitor cache.

Examples

The following example creates a flow monitor named FLOW-MONITOR-1 and enters flow monitor configuration mode:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)#
```

flow record

To create a flow record, or to modify an existing flow record, and enter flow record configuration mode, use the **flow record** command in global configuration mode. To remove a record, use the **no** form of this command.

flow record *record-name*
no flow record *record-name*

Syntax Description

record-name	Name of the flow record that is being created or modified.

Command Default

A flow record is not configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

A flow record defines the keys that uses to identify packets in the flow, as well as other fields of interest that gathers for the flow. You can define a flow record with any combination of keys and fields of interest. The switch supports a rich set of keys. A flow record also defines the types of counters gathered per flow. You can configure 64-bit packet or byte counters.

Examples

The following example creates a flow record named FLOW-RECORD-1, and enters flow record configuration mode:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)#
```

ftp-path

To configure the path at the FTP server for trace log export, use the **ftp-path** command. Use the **no** form of the command to negate the command or to set the command to its default.

`ftp-path`*ftp-path*

`no ftp-path`*ftp-path*

Syntax Description

ftp-path	Specifies the path at the FTP server.

Command Default

None

Command Modes

Wireless trace export profile FTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode ftp
Device(config-wireless-trace-export-profile-ftp)# ftp-path
ip-address/download/object/stream/images/ap-images
```

ftp-password

To configure the FTP server password for trace export, use the **ftp-password** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

`ftp-password}`<*Enter password*> <*Re-enter password*>

`no ftp-password`<*Enter password*> <*Re-enter password*>

Syntax Description

password	Specifies the FTP server password.
re-enter password	Indicates that the user must re-enter the FTP server password.

Command Default

None

Command Modes

Wireless trace export profile FTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode ftp
Device(config-wireless-trace-export-profile-ftp)# ftp-password xxxxxxxx xxxxxxxx
```

ftp-server

To configure the FTP server address for trace export, use the **ftp-server** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
ftp-server {A.B.C.D | X:X:X:X::X}

no ftp-server {A.B.C.D | X:X:X:X::X}
```

Syntax Description

A.B.C.D	Specifies the FTP IPv4 server address.
X:X:X:X::X	Specifies the FTP IPv6 server address.

Command Default

None

Command Modes

Wireless trace export profile FTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode ftp
Device(config-wireless-trace-export-profile-ftp)# ftp-server 10.1.1.1
```

ftp-username

To configure the FTP server username for trace export, use the **ftp-username**command. Use the **no** form of this command to negate the configuration or to set the command to its default.

`ftp-username` *Username*

`no ftp-username` *Username*

Syntax Description

username	Specifies the FTP server username.

Command Default

None

Command Modes

Wireless trace export profile FTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode ftp
Device(config-wireless-trace-export-profile-ftp)# ftp-username ftp-server-username
```

Configuration Commands: g to z

idle-timeout

To configure the idle-timeout value in seconds for a wireless profile policy, use the **idle-timeout** command.

idle-timeout *value*

Syntax Description

value	Sets the idle-timeout value. Valid range is 15 to 100000 seconds.

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to set the idle-timeout in a wireless profile policy:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-profile-name
Device(config-wireless-policy)# idle-timeout 100
```

image-download-mode

To configure image download using the HTTP, SFTP, TFTP, or CCO modes, use the **image-download-mode** command.

image-download-mode { **http** | **sftp** | **tftp** | **cco** }

Syntax Description

http	Configures image download using the HTTP mode.
sftp	Configures image download using the SFTP mode.
tftp	Configures image download using the TFTP mode.
cco	Configures image download using the CCO mode.

Command Default

None

Command Modes

Wireless image download profile configuration mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.
Cisco IOS XE Amsterdam 17.1.1s	The **image-download-mode cco**was introduced.

Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode http
```

inactive-timeout

To enable in-active timer, use the **inactive-timeout** command.

inactive-timeout *timeout-in-seconds*

Syntax Description

timeout-in-seconds	Specifies the inactive flow timeout value. The range is from 1 to 604800.

Command Default

None

Command Modes

ET-Analytics configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to enable in-active timer in the ET-Analytics configuration mode:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# et-analytics
Device(config-et-analytics)# inactive-timeout 15
Device(config-et-analytics)# end
```

install add file tftp

To install a package file to the system, use the **install add file tftp** command.

install add file tftp: *tftp file path*

Syntax Description

install add file tftp:	The **install add** command copies the file from the external server to the backup_image directory on the embedded wireless controller.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

Example

This example shows how to install a package file to the system:

```
Device#install add file tftp://<server-ip>/<path>/<smu-filename>
```

install add profile default

To download the embedded wireless controller image from the external server, use the **install add profile default** command.

install add profile *profile_name***activatecommitprompt-level none**

Syntax Description

add	Installs a package file to the system.
profile	Selects a profile.
profile_name	Adds a profile name with a maximum of 15 characters. Specify **default** to trigger the default behaviour.
activate	Activates the installed profile.
commit	Commits the changes to the loadpath.
prompt-level	Sets the prompt-level to none.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Usage Guidelines

Ensure that you have the *image-download-profile* configured on embedded wireless controller. Extract the contents of the image bundle (.zip archive) to an external TFTP or HTTP(S) server. The .zip archive contains the controller image and various compatible AP images (`apXgY`).

Example

The following example shows how to download the embedded wireless controller image:

```
Device#install add profile default

install_add: START Thu Jan 24 20:08:01 UTC 2019
Jan 24 20:08:03.389: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
add
Jan 24 20:08:03.389 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
add
install_add: Default profile addition successful
SUCCESS: install_add Thu Jan 24 20:08:03 UTC 2019
Jan 24 20:08:04.358: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install add
Jan 24 20:08:04.358 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install add
WLC#
*Jan 24 20:08:03.350: %INSTALL-5-INSTALL_START_INFO: Chassis 1 R0/0: install_engine: Started
 install add
```

```
*Jan 24 20:08:04.335: %INSTALL-5-INSTALL_COMPLETED_INFO: Chassis 1 R0/0: install_engine:
Completed install add
```

Note The log `Completed install add` means that the command is successful and the download will start soon.

The following example verifies the the image download status:

```
Device#sh wireless ewc-ap predownload status
```

install activate

To activate an installed package, use the **install activate** command.

install activate {**auto-abort-timer** | **file** | **profile** | **prompt-level**}

Syntax Description

auto-abort-timer	Sets the cancel timer. The time range is between 30 and 1200 minutes.
file	Specifies the package to be activated.
profile	Specifies the profile to be activated.
prompt-level	Sets the prompt level.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

The following example shows how to activate the installed package:

```
Device# install activate profile default
install_activate: START Thu Nov 24 20:14:53 UTC 2019

System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q] y
Building configuration...
[OK]Modified configuration has been saved
Jan 24 20:15:02.745: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
activate
Jan 24 20:15:02.745 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
activate
install_activate: Activating PACKAGE
```

install activate auto-abort-timer

To set the abort timer, use the **install activate auto-abort-timer** command.

install activate auto-abort-timer *<30-1200>* **prompt-level none**

Syntax Description

auto-abort-timer	Sets the cancel timer. The time range is between 30 and 1200 minutes.
<30-1200>	Specifies the cancel timer time in minutes.
prompt-level	Specifies the prompt level.
none	Specifies no prompting.

Command Default

None

Command Modes

Privileged EXEC (#)

Task ID

Task ID	Operation
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

The following example shows how to activate the cancel timer:

```
Device#install activate auto-abort-timer 30 prompt-level none
```

install activate file

To activate an installed package, use the **install activate file** command.

install activate file *file-name*

Syntax Description

file-name	Specifies the package name. Options are: bootflash:, flash:, and webui:.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Example

The following example shows how to use an auto cancel timer while activating an install package on a standby location:

```
Device# install activate file vwlc_apsp_16.11.1.0_74.bin
```

install auto-abort-timer stop

To stop the auto abort timer, use the **install auto-abort-timer stop** command.

install auto-abort-timer stop

Syntax Description

auto-abort-timer stop	Stops the auto-abort-timer

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

Example

This example shows how to stop the auto abort timer:

```
Device#install auto-abort-timer stop
```

install commit

To commit the changes to the loadpath, use the **install commit** command.

install commit

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

The following example shows how to commit the changes to the loadpath:

```
Device# install commit
```

install remove file backup_image

To remove installed packages, use the **install remove file backup_image** command.

install remove file backup_image *filename*

Syntax Description

filename	Specifes the file that needs to be removed.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

Example

This example shows how a file is removed from the package:

```
Device#install remove file backup_image: file_name
```

install remove profile default

To specify an install package that is to be removed, use the **install remove profile default** command.

install remove profile default

Syntax Description

remove	Removes the install package.
profile	Specifies the profile to be removed.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Example

The following example shows how to remove a default profile:

```
Device# install remove profile default
```

install deactivate

To specify an install package that is to be deactivated, use the **install deactivate file** command.

install deactivate file *file-name*

Syntax Description

file-name	Specifies the package name. Options are: bootflash:, flash:, and webui:.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Example

The following example shows how to deactivate an install package:

```
Device# install deactivate file vwlc_apsp_16.11.1.0_74.bin
```

install rollback

To roll back to a particular installation point, use the **install rollback** command.

install rollback to {**base** | **committed** | **id** *id* | **label** *label*} [**prompt-level none**]

Syntax Description

base	Rolls back to the base image.
prompt-level none	Sets the prompt level as none.
committed	Rolls back to the last committed installation point.
id	Rolls back to a specific install point ID.
label	Rolls back to a specific install point label.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Example

The following example shows how to specify the ID of the install point to roll back to:

```
Device# install rollback to id 1
```

interface vlan

To create or access a dynamic switch virtual interface (SVI) and to enter interface configuration mode, use the **interface vlan** command in global configuration mode. To delete an SVI, use the **no** form of this command.

interface vlan *vlan-id*
no interface vlan *vlan-id*

Syntax Description

vlan-id	VLAN number. The range is 1 to 4094.

Command Default

The default VLAN interface is VLAN 1.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

SVIs are created the first time you enter the **interface vlan** *vlan-id* command for a particular VLAN. The *vlan-id* corresponds to the VLAN-tag associated with data frames on an IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port.

Note When you create an SVI, it does not become active until it is associated with a physical port.

If you delete an SVI using the **no interface vlan** *vlan-id* command, it is no longer visible in the output from the **show interfaces** privileged EXEC command.

Note You cannot delete the VLAN 1 interface.

You can reinstate a deleted SVI by entering the **interface vlan** *vlan-id* command for the deleted interface. The interface comes back up, but the previous configuration is gone.

The interrelationship between the number of SVIs configured on a and the number of other features being configured might have an impact on CPU utilization due to hardware limitations. You can use the **sdm prefer** global configuration command to reallocate system hardware resources based on templates and feature tables.

You can verify your setting by entering the **show interfaces** and **show interfaces vlan** *vlan-id* privileged EXEC commands.

This example shows how to create a new SVI with VLAN ID 23 and enter interface configuration mode:

```
Device(config)# interface vlan 23
Device(config-if)#
```

ip access-group

To configure WLAN access control group (ACL), use the **ip access-group** command. To remove a WLAN ACL group, use the **no** form of the command.

ip access-group [**web**] *acl-name*
no ip access-group [**web**]

Syntax Description

web	(Optional) Configures the IPv4 web ACL.
acl-name	Specify the preauth ACL used for the WLAN with the security type value as webauth.

Command Default

None

Command Modes

WLAN configuration

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure a WLAN ACL:

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wlan wlan1
Device(config-wlan)#ip access-group test-acl
```

This example shows how to configure an IPv4 WLAN web ACL:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# ip access-group web test
Device(config-wlan)#
```

ip access-list extended

To configure extended access list, use the **ip access-list extended** command.

ip access-list extended {**<100-199>** | **<2000-2699>** *access-list-name*}

Syntax Description

<100-199>	Extended IP access-list number.
<2000-2699>	Extended IP access-list number (expanded range).

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure extended access list:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip access-list extended access-list-name
```

ip address

To set a primary or secondary IP address for an interface, use the **ip address** command in interface configuration mode. To remove an IP address or disable IP processing, use the noform of this command.

ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
no ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

Syntax Description

ip-address	IP address.
mask	Mask for the associated IP subnet.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. **Note** If the secondary address is used for a VRF table configuration with the **vrf** keyword, the **vrf** keyword must be specified also.
vrf	(Optional) Name of the VRF table. The *vrf-name* argument specifies the VRF name of the ingress interface.

Command Default

No IP address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all devices and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Devices respond to this request with an ICMP mask reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need 300 host addresses. Using

secondary IP addresses on the devices or access servers allows you to have two logical subnets using one physical subnet.

- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, device-based network. Devices on an older, bridged segment can be easily made aware that many subnets are on that segment.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.

Note

- If any device on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.
- When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.
- If you configure a secondary IP address, you must disable sending ICMP redirect messages by entering the **no ip redirects** command, to avoid high CPU utilization.

Examples

In the following example, 192.108.1.27 is the primary address and 192.31.7.17 is the secondary address for GigabitEthernet interface 1/0/1:

```
Device# enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 192.108.1.27 255.255.255.0
Device(config-if)# ip address 192.31.7.17 255.255.255.0 secondary
```

Related Commands

Command	Description
match ip route-source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show ip interface	Displays the usability status of interfaces configured for IP.
show route-map	Displays static and dynamic route maps.

ip dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) address pool on a DHCP server and enter DHCP pool configuration mode, use the **ip dhcp pool** command in global configuration mode. To remove the address pool, use the no form of this command.

ip dhcp pool *name*
no ip dhcp pool *name*

Syntax Description

name	Name of the pool. Can either be a symbolic string (such as engineering) or an integer (such as 0).

Command Default

DHCP address pools are not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

During execution of this command, the configuration mode changes to DHCP pool configuration mode, which is identified by the (config-dhcp)# prompt. In this mode, the administrator can configure pool parameters, like the IP subnet number and default router list.

Examples

The following example configures pool1 as the DHCP address pool:

```
ip dhcp pool pool1
```

Related Commands

Command	Description
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp excluded-address	Specifies IP addresses that a Cisco IOS DHCP server should not assign to DHCP clients.
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.

ip dhcp-relay information option server-override

To enable the system to globally insert the server ID override and link selection suboptions into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a Dynamic Host Configuration Protocol (DHCP) server, use the **ip dhcp-relay information option server-override** command in global configuration mode. To disable inserting the server ID override and link selection suboptions into the DHCP relay agent information option, use the **no** form of this command.

ip dhcp-relay information option server-override
no ip dhcp-relay information option server-override

Syntax Description

This command has no arguments or keywords.

Command Default

The server ID override and link selection suboptions are not inserted into the DHCP relay agent information option.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **ip dhcp-relay information option server-override** command adds the following suboptions into the relay agent information option when DHCP broadcasts are forwarded by the relay agent from clients to a DHCP server:

- Server ID override suboption
- Link selection suboption

When this command is configured, the gateway address (giaddr) will be set to the IP address of the outgoing interface, which is the interface that is reachable by the DHCP server.

If the **ip dhcp relay information option server-id-override** command is configured on an interface, it overrides the global configuration on that interface only.

Examples

In the following example, the DHCP relay will insert the server ID override and link selection suboptions into the relay information option of the DHCP packet. The loopback interface IP address is configured to be the source IP address for the relayed messages.

```
Device(config)# ip dhcp-relay information option server-override
Device(config)# ip dhcp-relay source-interface loopback 0
Device(config)# interface Loopback 0
Device(config-if)# ip address 10.2.2.1 255.255.255.0
```

Related Commands

Command	Description
ip dhcp relay information option server-id-override	Enables the system to insert the server ID override and link selection suboptions on a specific interface into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.

ip dhcp-relay source-interface

To globally configure the source interface for the relay agent to use as the source IP address for relayed messages, use the **ip dhcp-relay source-interface** command in global configuration mode. To remove the source interface configuration, use the **no** form of this command.

ip dhcp-relay source-interface *type number*
no ip dhcp-relay source-interface *type number*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering system for your networking device, use the question mark (?) online help function.

Command Default

The source interface is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **ip dhcp-relay source-interface** command allows the network administrator to specify a stable, hardware-independent IP address (such as a loopback interface) for the relay agent to use as a source IP address for relayed messages.

If the **ip dhcp-relay source-interface** global configuration command is configured and the **ip dhcp relay source-interface** command is also configured, the **ip dhcp relay source-interface** command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.

Examples

In the following example, the loopback interface IP address is configured to be the source IP address for the relayed messages:

```
Device(config)# ip dhcp-relay source-interface loopback 0
Device(config)# interface loopback 0
Device(config-if)# ip address 10.2.2.1 255.255.255.0
```

Related Commands

Command	Description
ip dhcp relay source-interface	Configures the source interface for the relay agent to use as the source IP address for relayed messages.

ip domain-name

To configure the host domain on the device, use the **ip domain-name** command.

ip domain-name *domain-name* [**vrf** *vrf-name*]

Syntax Description

domain-name	Default domain name.
vrf-name	Specifies the virtual routing and forwarding (VRF) to use to resolve the domain name.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure a host domain in a device:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip domain-name domain-name
```

ip flow monitor

To configure IP NetFlow monitoring, use the **ip flow monitor** command. To remove IP NetFlow monitoring, use the **no** form of this command.

ip flow monitor *ip-monitor-name* {**input** | **output**}
no ip flow monitor *ip-monitor-name* {**input** | **output**}

Syntax Description

ip-monitor-name	Flow monitor name.
input	Enables a flow monitor for ingress traffic.
output	Enables a flow monitor for egress traffic.

Command Default

None

Command Modes

WLAN configuration

Usage Guidelines

You must disable the WLAN before using this command.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure an IP flow monitor for the ingress traffic:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# ip flow monitor test input
```

This example shows how to disable an IP flow monitor:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no ip flow monitor test input
```

ip flow-export destination

To configure ETA flow export destination, use the **ip flow-export destination** command.

ip flow-export destination *ip_address port_number*

Syntax Description

port_number	Port number. The range is from 1 to 65535.

Command Default

None

Command Modes

ET-Analytics configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure ETA flow export destination in the ET-Analytics configuration mode:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# et-analytics
Device(config-et-analytics)# ip flow-export
destination 120.0.0.1 2055
Device(config-et-analytics)# end
```

ip helper-address

To enable forwarding of User Datagram Protocol (UDP) broadcasts, including Bootstrap Protocol (BOOTP), received on an interface, use the **ip helper-address** command in interface configuration mode. To disable forwarding of broadcast packets to specific addresses, use the**no** form of this command.

ip helper-address[{**vrf** *name* | **global**}] *address* {[**redundancy** *vrg-name*]}
no ip helper-address [{**vrf** *name* | **global**}] *address* {[**redundancy** *vrg-name*]}

Syntax Description

vrf *name*	(Optional) Enables the VPN routing and forwarding (VRF) instance and the VRF name.
global	(Optional) Configures a global routing table.
address	Destination broadcast or host address to be used when forwarding UDP broadcasts. There can be more than one helper address per interface.
redundancy *vrg-name*	(Optional) Defines the Virtual Router Group (VRG) name.

Command Default

UDP broadcasts are not forwarded.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(4)B	This command was modified. The **vrf** *name* keyword and argument pair and the **global** keyword were added.
12.2(15)T	This command was modified. The **redundancy** *vrg-name* keyword and argument pair was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip forward-protocol** command along with the **ip helper-address** command allows you to control broadcast packets and protocols that are forwarded.

One common application that requires helper addresses is DHCP, which is defined in RFC 1531. To enable BOOTP or DHCP broadcast forwarding for a set of clients, configure a helper address on the router interface connected to the client. The helper address must specify the address of the BOOTP or DHCP server. If you have multiple servers, configure one helper address for each server.

The following conditions must be met for a UDP or IP packet to be able to use the **ip helper-address** command:

- The MAC address of the received frame must be all-ones broadcast address (ffff.ffff.ffff).

- The IP destination address must be one of the following: all-ones broadcast (255.255.255.255), subnet broadcast for the receiving interface, or major-net broadcast for the receiving interface if the **no ip classless** command is also configured.
- The IP time-to-live (TTL) value must be at least 2.
- The IP protocol must be UDP (17).
- The UDP destination port must be for TFTP, Domain Name System (DNS), Time, NetBIOS, ND, BOOTP or DHCP packet, or a UDP port specified by the **ip forward-protocol udp** command in global configuration mode.

If the DHCP server resides in a VPN or global space that is different from the interface VPN, then the **vrf** *name* or the **global** option allows you to specify the name of the VRF or global space in which the DHCP server resides.

The **ip helper-addressvrf***name address* option uses the address associated with the VRF name regardless of the VRF of the incoming interface. If the **ip helper-addressvrf***name address* command is configured and later the VRF is deleted from the configuration, then all IP helper addresses associated with that VRF name will be removed from the interface configuration.

If the **ip helper-address** *address* command is already configured on an interface with no VRF name configured, and later the interface is configured with the **ip helper-address vrf** *name address* command, then the previously configured **ip helper-address** *address* command is considered to be global.

Note The **ip helper-address**command does not work on an X.25 interface on a destination router because the router cannot determine if the packet was intended as a physical broadcast.

The **service dhcp** command must be configured on the router to enable IP helper statements to work with DHCP. If the command is not configured, the DHCP packets will not be relayed through the IP helper statements. The **service dhcp** command is configured by default.

Examples

The following example shows how to define an address that acts as a helper address:

```
Router(config)# interface ethernet 1
Router(config-if)# ip helper-address 10.24.43.2
```

The following example shows how to define an address that acts as a helper address and is associated with a VRF named host1:

```
Router(config)# interface ethernet 1/0
Router(config-if)# ip helper-address vrf host1 10.25.44.2
```

The following example shows how to define an address that acts as a helper address and is associated with a VRG named group1:

```
Router(config)# interface ethernet 1/0
Router(config-if)# ip helper-address 10.25.45.2 redundancy group1
```

Related Commands

Command	Description
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.
service dhcp	Enables the DHCP server and relay agent features on the router.

ip http client secure-ciphersuite

To specify the CipherSuite that should be used for encryption over the secure HTTP connection from the client to a remote server, use the **ip http client secure-ciphersuite** command in global configuration mode. To remove a previously configured CipherSuite specification for the client, use the **no** form of this command.

ip http client secure-ciphersuite [**3des-ede-cbc-sha**] [**rc4-128-sha**] [**rc4-128-md5**] [**des-cbc-sha**]
no ip http client secure-ciphersuite

Syntax Description

3des-ede-cbc-sha	SSL_RSA_WITH_3DES_EDE_CBC_SHA--Rivest, Shamir, and Adleman (RSA) key exchange with 3DES and DES-EDE3-CBC for message encryption and Secure Hash Algorithm (SHA) for message digest.
rc4-128-sha	SSL_RSA_WITH_RC4_128_SHA--RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and SHA for message digest.
rc4-128-md5	SSL_RSA_WITH_RC4_128_MD5--RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and Message Digest 5 (MD5) for message digest.
des-cbc-sha	SSL_RSA_WITH_DES_CBC_SHA--RSA key exchange with DES-CBC for message encryption and SHA for message digest.

Command Default

The client and server negotiate the best CipherSuite that they both support from the list of available CipherSuites.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE

Usage Guidelines

This command allows you to restrict the list of CipherSuites (encryption algorithms) that the client offers when connecting to a secure HTTP server. For example, you may want to allow only the most secure CipherSuites to be used.

Unless you have a reason to specify the CipherSuites that should be used, or you are unfamiliar with the details of these CipherSuites, you should leave this command unconfigured and let the server and client negotiate the CipherSuite that they both support (this is the default). The **no** form of this command returns the list of available CipherSuites to the default (that is, all CipherSuites supported on your device are available for negotiation).

Examples

The following example shows how to configure the HTTPS client to use only the SSL_RSA_WITH_3DES_EDE_CBC_SHA CipherSuite:

```
Router(config)# ip http client secure-ciphersuite 3des-ede-cbc-sha
```

ip http secure-ciphersuite

To specify the CipherSuites that should be used by the secure HTTP server when negotiating a connection with a remote client, use the **ip http secure-ciphersuite** command in global configuration mode. To return the configuration to the default set of CipherSuites, use the **no** form of this command.

ip http secure-ciphersuite [**3des-ede-cbc-sha**] [**rc4-128-sha**] [**rc4-128-md5**] [**des-cbc-sha**]
no ip http secure-ciphersuite

Syntax Description

3des-ede-cbc-sha	SSL_RSA_WITH_3DES_EDE_CBC_SHA--Rivest, Shamir, and Adleman (RSA) key exchange with 3DES and DES-EDE3-CBC for message encryption and Secure Hash Algorithm (SHA) for message digest.
rc4-128-sha	SSL_RSA_WITH_RC4_128_SHA --RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and SHA for message digest.
rc4-128-md5	SSL_RSA_WITH_RC4_128_MD5 --RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and Message Digest 5 (MD5) for message digest.
des-cbc-sha	SSL_RSA_WITH_DES_CBC_SHA--RSA key exchange with DES-CBC for message encryption and SHA for message digest.

Command Default

The HTTPS server negotiates the best CipherSuite using the list received from the connecting client.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE

Usage Guidelines

This command is used to restrict the list of CipherSuites (encryption algorithms) that should be used for encryption over the HTTPS connection. For example, you may want to allow only the most secure CipherSuites to be used.

Unless you have a reason to specify the CipherSuites that should be used, or you are unfamiliar with the details of these CipherSuites, you should leave this command unconfigured and let the server and client negotiate the CipherSuite that they both support (this is the default).

The supported CipherSuites vary by Cisco IOS software image. For example, “IP Sec56” (“k8”) images support only the SSL_RSA_WITH_DES_CBC_SHA CipherSuite in Cisco IOS Release 12.2(15)T.

In terms of router processing load (speed), the following list ranks the CipherSuites from fastest to slowest (slightly more processing time is required for the more secure and more complex CipherSuites):

1. SSL_RSA_WITH_DES_CBC_SHA
2. SSL_RSA_WITH_RC4_128_MD5
3. SSL_RSA_WITH_RC4_128_SHA

4. SSL_RSA_WITH_3DES_EDE_CBC_SHA

Additional information about these CipherSuites can be found online from sources that document the Secure Sockets Layer (SSL) 3.0 protocol.

Examples

The following exampleshows how to restrictsthe CipherSuites offered to a connecting secure web client:

```
Router(config)# ip http secure-ciphersuite rc4-128-sha rc4-128-md5
```

ip http secure-server

To enable a secure HTTP (HTTPS) server, enter the **ip http secure-server** command in global configuration mode. To disable the HTTPS server, use the **no** form of this command..

ip http secure-server
no ip http secure-server

Syntax Description

This command has no arguments or keywords.

Command Default

The HTTPS server is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

The HTTPS server uses the Secure Sockets Layer (SSL) version 3.0 protocol.

⚠

Caution When enabling an HTTPS server, you should always disable the standard HTTP server to prevent unsecured connections to the same services. Disable the standard HTTP server using the **no ip http server** command in global configuration mode (this step is precautionary; typically, the HTTP server is disabled by default).

If a certificate authority (CA) is used for certification, you should declare the CA trustpoint on the routing device before enabling the HTTPS server.

To close HTTP/TCP port 8090, you must disable both the HTTP and HTTPS servers. Enter the **no http server** and the **no http secure-server** commands, respectively.

Examples

In the following example the HTTPS server is enabled, and the (previously configured) CA trustpoint CA-trust-local is specified:

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ip http secure-server
Device(config)#ip http secure-trustpoint CA-trust-local
Device(config)#end

Device#show ip http server secure status
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: CA-trust-local
```

Related Commands

Command	Description
ip http secure-trustpoint	Specifies the CA trustpoint that should be used for obtaining signed certificates for the HTTPS server.
ip http server	Enables the HTTP server on an IP or IPv6 system, including the Cisco web browser user interface.
show ip http server secure status	Displays the configuration status of the HTTPS server.

ip http server

To enable the HTTP server on your IP or IPv6 system, including the Cisco web browser user interface, enter the **ip http server** command in global configuration mode. To disable the HTTP server, use the **no** form of this command..

ip http server
no ip http server

Syntax Description

This command has no arguments or keywords.

Command Default

The HTTP server uses the standard port 80 by default.

HTTP/TCP port 8090 is open by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The command enables both IPv4 and IPv6 access to the HTTP server. However, an access list configured with the **ip http access-class** command is applied only to IPv4 traffic. IPv6 traffic filtering is not supported.

Caution The standard HTTP server and the secure HTTP (HTTPS) server can run on a system at the same time. If you enable the HTTPS server using the **ip http secure-server** command, disable the standard HTTP server using the **no ip http server** command to ensure that secure data cannot be accessed through the standard HTTP connection.

To close HTTP/TCP port 8090, you must disable both the HTTP and HTTPS servers. Enter the **no http server** and the **no http secure-server** commands, respectively.

Examples

The following example shows how to enable the HTTP server on both IPv4 and IPv6 systems.

After enabling the HTTP server, you can set the base path by specifying the location of the HTML files to be served. HTML files used by the HTTP web server typically reside in system flash memory. Remote URLs can be specified using this command, but use of remote path names (for example, where HTML files are located on a remote TFTP server) is not recommended.

```
Device(config)#ip http server
Device(config)#ip http path flash:
```

Related Commands

Command	Description
ip http access-class	Specifies the access list that should be used to restrict access to the HTTP server.
ip http path	Specifies the base path used to locate files for use by the HTTP server.

Command	Description
ip http secure-server	Enables the HTTPS server.

ip ssh

To configure Secure Shell (SSH) control parameters on your router, use the **ip ssh** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip ssh [{**timeout** *seconds* | **authentication-retries** *integer*}]
no ip ssh [{**timeout** *seconds* | **authentication-retries** *integer*}]

Syntax Description

timeout	(Optional) The time interval that the router waits for the SSH client to respond. This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply. By default, there are 5 vtys defined (0-4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes.
seconds	(Optional) The number of seconds until timeout disconnects, with a maximum of 120 seconds. The default is 120 seconds.
authentication- retries	(Optional) The number of attempts after which the interface is reset.
integer	(Optional) The number of retries, with a maximum of 5 authentication retries. The default is 3.

Command Default

SSH control parameters are set to default router values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1) T.
12.2(17a)SX	This command was integrated into Cisco IOS Release 12.2(17a)SX.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

Before you configure SSH on your router, you must enable the SSH server using the **crypto key generate rsa**command.

Examples

The following examples configure SSH control parameters on your router:

```
ip ssh timeout 120
ip ssh authentication-retries 3
```

ip ssh version

To specify the version of Secure Shell (SSH) to be run on a router, use the **ip ssh version**command in global configuration mode. To disable the version of SSH that was configured and to return to compatibility mode, use the **no** form of this command.

ip ssh version [{**1** | **2**}]
no ip ssh version [{**1** | **2**}]

Syntax Description

1	(Optional) Router runs only SSH Version 1.
2	(Optional) Router runs only SSH Version 2.

Command Default

If this command is not configured, SSH operates in compatibility mode, that is, Version 1 and Version 2 are both supported.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(7)JA	This command was integrated into Cisco IOS Release 12.3(7)JA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

You can use this command with the **2** keyword to ensure that your router will not inadvertently establish a weaker SSH Version 1 connection.

Examples

The following example shows that only SSH Version 1 support is configured:

```
Router (config)# ip ssh version 1
```

The following example shows that only SSH Version 2 is configured:

```
Router (config)# ip ssh version 2
```

The following example shows that SSH Versions 1 and 2 are configured:

```
Router (config)# no ip ssh version
```

Related Commands

Command	Description
debug ip ssh	Displays debug messages for SSH.
disconnect ssh	Terminates a SSH connection on your router.
ip ssh	Configures SSH control parameters on your router.
ip ssh rsa keypair-name	Specifies which RSA key pair to use for a SSH connection.
show ip ssh	Displays the SSH connections of your router.

ip tftp blocksize

To specify TFTP client blocksize, use the **ip tftp blocksize** command.

ip tftp blocksize *blocksize-value*

Syntax Description

blocksize-value	Blocksize value. Valid range is from 512-8192 Kbps.

Command Default

TFTP client blocksize is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

Use this command to change the default blocksize to decrease the image download time.

Example

The following example shows how to specify TFTP client blocksize:

```
Device(config)# ip tftp blocksize 512
```

ip verify source

To enable IP source guard on an interface, use the **ip verify source** command in interface configuration mode. To disable IP source guard, use the **no** form of this command.

ip verify source
no ip verify source

Command Default

IP source guard is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

To enable IP source guard with source IP address filtering, use the **ip verify source** interface configuration command.

Examples

This example shows how to enable IP source guard with source IP address filtering on an interface:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source
```

You can verify your settings by entering the **show ip verify source** privileged EXEC command.

ipv4 acl

To create ACL configuration for wireless IPv4, use the **ipv4 acl** command.

configuration.

ipv4 acl *ipv4-acl-name*

Syntax Description

ipv4 acl	Creates ACL configuration for wireless IPv4.
ipv4-acl-name	Specifies the IPv4 ACL name.

Command Default

None

Command Modes

Wireless policy confirguration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

Example

This example shows how to create an ACL configuration for wireless IPv4:

```
Device(config-wireless-policy)#ipv4 acl ipv4-acl-name
```

ipv4 dhcp

To configure the DHCP parameters for a WLAN, use the **ipv4 dhcp** command.

ipv4 dhcp {**opt82** | {**ascii** | **rid** | **format** | {**ap_ethmac** | **ap_location** | **apmac** | **apname** | **policy_tag** | **ssid** | **vlan_id** }} | **required** | **server** *dhcp-ip-addr*}

Syntax Description

opt82	Sets DHCP option 82 for wireless clients on this WLAN
required	Specifies whether DHCP address assignment is required
server	Configures the WLAN's IPv4 DHCP Server
ascii	Supports ASCII for DHCP option 82
rid	Supports adding Cisco 2 byte RID for DHCP option 82
format	Sets RemoteID format
ap_ethmac	Enables DHCP AP Ethernet MAC address
ap_location	Enables AP location
apmac	Enables AP MAC address
apname	Enables AP name
policy_tag	Enables Policy tag
ssid	Enables SSID
vlan_id	Enables VLAN ID
dhcp-ip-addr	Enter the override DHCP server's IP Address.

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure DHCP address assignment as a requirement:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy demo-profile-name
Device(config-wireless-policy)# ipv4 dhcp required
```

ipv4 flow monitor

To configure the IPv4 traffic ingress flow monitor for a WLAN profile policy, use the **ipv4 flow monitor input** command.

ipv4 flow monitor *monitor-name* **input**

Syntax Description

monitor-name	Flow monitor name.
input	Enables flow monitor on ingress traffic.

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the IPv4 traffic ingress flow monitor for a WLAN profile policy:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-profile-name
Device(config-wireless-policy)# ipv4 flow monitor flow-monitor-name input
```

ipv4 flow monitor output

To configure the IPv4 traffic egress flow monitor for a WLAN profile policy, use the **ipv4 flow monitor output** command.

ipv4 flow monitor *monitor-name* **output**

Syntax Description

monitor-name	Flow monitor name.
output	Enables flow monitor on egress traffic.

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.2.1.

Examples

The following example shows how to configure the IPv4 traffic egress flow monitor for a WLAN profile policy:

```
Device(config-wireless-policy)#ipv4 flow monitor flow-monitor-name output
```

ipv6 flow monitor input

To configure the IPv6 traffic ingress flow monitor for a WLAN profile policy, use the **ipv6 flow monitor input** command.

ipv6 flow monitor *monitor-name* **input**

Syntax Description

monitor-name	Flow monitor name.
input	Enables flow monitor on ingress traffic.

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.2.1.

Examples

The following example shows how to configure the IPv6 traffic ingress flow monitor for a WLAN profile policy:

```
Device(config-wireless-policy)#ipv6 flow monitor flow-monitor-name input
```

ipv6 flow monitor output

To configure the IPv6 traffic egress flow monitor for a WLAN profile policy, use the **ipv6 flow monitor output** command.

ipv6 flow monitor *monitor-name* **output**

Syntax Description

monitor-name	Flow monitor name.
output	Enables flow monitor on egress traffic.

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.2.1.

Examples

The following example shows how to configure the IPv6 traffic egress flow monitor for a WLAN profile policy:

```
Device(config-wireless-policy)#ipv6 flow monitor flow-monitor-name output
```

ipv6 access-list

To define an IPv6 access list and to place the device in IPv6 access list configuration mode, use the **ipv6 access-list** command in global configuration mode. To remove the access list, use the **no** form of this command.

ipv6 access-list *access-list-name* | **match-local-traffic** | **log-update threshold** *threshold-in-msgs* | **role-based** *list-name*
noipv6 access-list *access-list-name* | **client** *permit-control-packets* | **log-update** *threshold* | **role-based** *list-name*

Syntax Description

ipv6 *access-list-name*	Creates a named IPv6 ACL (up to 64 characters in length) and enters IPv6 ACL configuration mode. *access-list-name* - Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.
match-local-traffic	Enables matching for locally-generated traffic.
log-update threshold *threshold-in-msgs*	Determines how syslog messages are generated after the initial packet match. *threshold-in-msgs*- Number of packets generated.
role-based *list-name*	Creates a role-based IPv6 ACL.

Command Default

No IPv6 access list is defined.

Command Modes

Global configuration

Command History

Release	Modification

Usage Guidelines

IPv6 ACLs are defined by using the **ipv6 access-list**command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit**commands in IPv6 access list configuration mode. Configuring the **ipv6 access-list**command places the device in IPv6 access list configuration mode--the device prompt changes to Device(config-ipv6-acl)#. From IPv6 access list configuration mode, permit and deny conditions can be set for the defined IPv6 ACL.

Note IPv6 ACLs are defined by a unique name (IPv6 does not support numbered ACLs). An IPv4 ACL and an IPv6 ACL cannot share the same name.

IPv6 is automatically configured as the protocol type in **permit any any** and **deny any any** statements that are translated from global configuration mode to IPv6 access list configuration mode.

Every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect. The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default,

IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Use the **ipv6 traffic-filter** interface configuration command with the *access-list-name* argument to apply an IPv6 ACL to an IPv6 interface. Use the **ipv6 access-class** line configuration command with the *access-list-name* argument to apply an IPv6 ACL to incoming and outgoing IPv6 virtual terminal connections to and from the device.

An IPv6 ACL applied to an interface with the **ipv6 traffic-filter** command filters traffic that is forwarded, not originated, by the device.

Examples

The example configures the IPv6 ACL list named list1 and places the device in IPv6 access list configuration mode.

```
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)#
```

The following example configures the IPv6 ACL named list2 and applies the ACL to outbound traffic on Ethernet interface 0. Specifically, the first ACL entry keeps all packets from the network FEC0:0:0:2::/64 (packets that have the site-local prefix FEC0:0:0:2 as the first 64 bits of their source IPv6 address) from exiting out of Ethernet interface 0. The second entry in the ACL permits all other traffic to exit out of Ethernet interface 0. The second entry is necessary because an implicit deny all condition is at the end of each IPv6 ACL.

```
Device(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Device(config)# ipv6 access-list list2 permit any any
Device(config)# interface ethernet 0
Device(config-if)# ipv6 traffic-filter list2 out
```

ipv6 acl

To create ACL configuration for wireless IPv6, use the **ipv6 acl** command.

configuration.

ipv6 acl *ipv6-acl-name*

Syntax Description

ipv6 acl	Creates ACL configuration for wireless IPv6.
ipv6-acl-name	Specifies the IPv6 ACL name.

Command Default

None

Command Modes

Wireless policy confirguration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

Example

This example shows how to create an ACL configuration for wireless IPv6:

```
Device(config-wireless-policy)#ipv6 acl ipv6-acl-name
```

ipv6-address-type

To configure the 802.11u IPv6 address type, use the **ipv6-address-type** command. To remove the address type, use the **no** form of the command.

ipv6-address-type {**available** | **not-available** | **not-known**}

Syntax Description

available	Sets IPv6 address type as available.
not-available	Sets IPv6 address type as not available.
not-known	Sets IPv6 address type availability as not known.

Command Default

None

Command Modes

Wireless ANQP Server Configuration (config-wireless-anqp-server)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Example

The following example shows how to configure a 802.11u IPv6 address type:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# ipv4-address-type available
```

ipv6 address

To configure an IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface, use the **ipv6 address**command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address {*ipv6-prefix/prefix-length* | *prefix-name sub-bits/prefix-length*}
no ipv6 address {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*}

Syntax Description

ipv6-address	The IPv6 address to be used.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
prefix-name	A general prefix, which specifies the leading bits of the network to be configured on the interface.
sub-bits	The subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the *prefix-name* argument. The *sub-bits*argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

No IPv6 addresses are defined for any interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco ASR 1000 Series devices.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 address** command allows multiple IPv6 addresses to be configured on an interface in various different ways, with varying options. The most common way is to specify the IPv6 address with the prefix length.

Addresses may also be defined using the general prefix mechanism, which separates the aggregated IPv6 prefix bits from the subprefix and host bits. In this case, the leading bits of the address are defined in a general prefix, which is globally configured or learned (for example, through use of Dynamic Host Configuration Protocol-Prefix Delegation (DHCP-PD)), and then applied using the *prefix-name* argument. The subprefix bits and host bits are defined using the *sub-bits* argument.

Using the **no ipv6 address autoconfig** command without arguments removes all IPv6 addresses from an interface.

IPv6 link-local addresses must be configured and IPv6 processing must be enabled on an interface by using the **ipv6 address link-local** command.

Examples

The following example shows how to enable IPv6 processing on the interface and configure an address based on the general prefix called my-prefix and the directly specified bits:

```
Device(config-if) ipv6 address my-prefix 0:0:0:7272::72/64
```

Assuming the general prefix named my-prefix has the value of 2001:DB8:2222::/48, then the interface would be configured with the global address 2001:DB8:2222:7272::72/64.

Related Commands

Command	Description
ipv6 address anycast	Configures an IPv6 anycast address and enables IPv6 processing on an interface.
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
no ipv6 address autoconfig	Removes all IPv6 addresses from an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 server configuration information pool and enter DHCP for IPv6 pool configuration mode, use the **ipv6 dhcp pool** command in global configuration mode. To delete a DHCP for IPv6 pool, use the **no** form of this command.

ipv6 dhcp pool *poolname*
no ipv6 dhcp pool *poolname*

Syntax Description

poolname	User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).

Command Default

DHCP for IPv6 pools are not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Use the **ipv6 dhcp pool**command to create a DHCP for IPv6 server configuration information pool. When the **ipv6 dhcp pool** command is enabled, the configuration mode changes to DHCP for IPv6 pool configuration mode. In this mode, the administrator can configure pool parameters, such as prefixes to be delegated and Domain Name System (DNS) servers, using the following commands:

- **address prefix** *IPv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}]sets an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons.
- **link-address** *IPv6-prefix* sets a link-address IPv6 prefix. When an address on the incoming interface or a link-address in the packet matches the specified IPv6-prefix, the server uses the configuration information pool. This address must be in hexadecimal, using 16-bit values between colons.
- **vendor-specific** *vendor-id* enables DHCPv6 vendor-specific configuration mode. Specify a vendor identification number. This number is the vendor IANA Private Enterprise Number. The range is 1 to 4294967295. The following configuration command is available:
  - **suboption** *number* sets vendor-specific suboption number. The range is 1 to 65535. You can enter an IPv6 address, ASCII text, or a hex string as defined by the suboption parameters.

Note The **hex** value used under the **suboption** keyword allows users to enter only hex digits (0-f). Entering an invalid **hex** value does not delete the previous configuration.

Once the DHCP for IPv6 configuration information pool has been created, use the **ipv6 dhcp server** command to associate the pool with a server on an interface. If you do not configure an information pool, you need to use the **ipv6 dhcp server interface** configuration command to enable the DHCPv6 server function on an interface.

When you associate a DHCPv6 pool with an interface, only that pool services requests on the associated interface. The pool also services other interfaces. If you do not associate a DHCPv6 pool with an interface, it can service requests on any interface.

Not using any IPv6 address prefix means that the pool returns only configured options.

The **link-address** command allows matching a link-address without necessarily allocating an address. You can match the pool from multiple relays by using multiple link-address configuration commands inside a pool.

Since a longest match is performed on either the address pool information or the link information, you can configure one pool to allocate addresses and another pool on a subprefix that returns only configured options.

Examples

The following example specifies a DHCP for IPv6 configuration information pool named cisco1 and places the router in DHCP for IPv6 pool configuration mode:

```
Router(config)# ipv6 dhcp pool cisco1
Router(config-dhcpv6)#
```

The following example shows how to configure an IPv6 address prefix for the IPv6 configuration pool cisco1:

```
Router(config-dhcpv6)# address prefix 2001:1000::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named engineering with three link-address prefixes and an IPv6 address prefix:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# link-address 2001:1001::0/64
Router(config-dhcpv6)# link-address 2001:1002::0/64
Router(config-dhcpv6)# link-address 2001:2000::0/48
Router(config-dhcpv6)# address prefix 2001:1003::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named 350 with vendor-specific options:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool 350
Router(config-dhcpv6)# vendor-specific 9
Router(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Router(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Router(config-dhcpv6-vs)# end
```

Related Commands

Command	Description
ipv6 dhcp server	Enables DHCP for IPv6 service on an interface.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

ipv6 enable

To enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **ipv6 enable**command in interface configuration mode. To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

ipv6 enable
no ipv6 enable

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

The **ipv6 enable**command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing. The no **ipv6 enable**command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

Examples

The following example enables IPv6 processing on Ethernet interface 0/0:

```
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 enable
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 mld snooping

To enable Multicast Listener Discovery version 2 (MLDv2) protocol snooping globally, use the **ipv6 mld snooping** command in global configuration mode. To disable the MLDv2 snooping globally, use the **no** form of this command.

ipv6 mld snooping
no ipv6 mld snooping

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

MLDv2 snooping is supported on the Supervisor Engine 720 with all versions of the Policy Feature Card 3 (PFC3).

To use MLDv2 snooping, configure a Layer 3 interface in the subnet for IPv6 multicast routing or enable the MLDv2 snooping querier in the subnet.

Examples

This example shows how to enable MLDv2 snooping globally:

```
Router(config)# ipv6 mld snooping
```

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 nd managed-config-flag

To set the managed address configuration flag in IPv6 router advertisements, use the **ipv6 nd managed-config-flag** command in an appropriate configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag

Syntax Description

This command has no keywords or arguments.

Command Default

The managed address configuration flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

Setting the managed address configuration flag in IPv6 router advertisements indicates to attached hosts whether they should use stateful autoconfiguration to obtain addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain addresses. If the flag is not set, the attached hosts should not use stateful autoconfiguration to obtain addresses.

Hosts may use stateful and stateless address autoconfiguration simultaneously.

Examples

This example shows how to configure the managed address configuration flag in IPv6 router advertisements:

```
Device(config)# interface
Device(config-if)# ipv6 nd managed-config-flag
```

ipv6 nd other-config-flag

To set the other stateful configuration flag in IPv6 router advertisements, use the **ipv6 nd other-config-flag** command in an appropriate configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd other-config-flag

Syntax Description

This command has no keywords or arguments.

Command Default

The other stateful configuration flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration

Dynamic template configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

The setting of the other stateful configuration flag in IPv6 router advertisements indicates to attached hosts how they can obtain autoconfiguration information other than addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain the other (nonaddress) information.

Note If the managed address configuration flag is set using the **ipv6 nd managed-config-flag** command, then an attached host can use stateful autoconfiguration to obtain the other (nonaddress) information regardless of the setting of the other stateful configuration flag.

Examples

This example (not applicable for BNG) configures the “other stateful configuration” flag in IPv6 router advertisements:

```
Device(config)# interface
Device(config-if)# ipv6 nd other-config-flag
```

ipv6 nd ra throttler attach-policy

To configure a IPv6 policy for feature RA throttler, use the **ipv6 nd ra-throttler attach-policy** command.

ipv6 nd ra-throttler attach-policy *policy-name*

Syntax Description

ipv6	IPv6 root chain.
ra-throttler	Configure RA throttler on the VLAN.
attach-policy	Apply a policy for feature RA throttler.
policy-name	Policy name for feature RA throttler

Command Default

None

Command Modes

config-vlan

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure configure a IPv6 policy for feature RA throttler:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# vlan configuration vlan-id
Device(config-vlan-config)# ipv6 nd ra-throttler attach-policy
```

ipv6 nd raguard policy

To define the router advertisement (RA) guard policy name and enter RA guard policy configuration mode, use the **ipv6 nd raguard policy** command in global configuration mode.

ipv6 nd raguardpolicy *policy-name*

Syntax Description

policy-name	IPv6 RA guard policy name.

Command Default

An RA guard policy is not configured.

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

Use the **ipv6 nd raguard policy** command to configure RA guard globally on a router. Once the device is in ND inspection policy configuration mode, you can use any of the following commands:

- **device-role**
- **drop-unsecure**
- **limit address-count**
- **sec-level minimum**
- **trusted-port**
- **validate source-mac**

After IPv6 RA guard is configured globally, you can use the **ipv6 nd raguard attach-policy** command to enable IPv6 RA guard on a specific interface.

Examples

The following example shows how to define the RA guard policy name as policy1 and place the device in policy configuration mode:

```
Device(config)# ipv6 nd raguard policy policy1
Device(config-ra-guard)#
```

Related Commands

Table 8:

Command	Description
device-role	Specifies the role of the device attached to the port.
drop-unsecure	Drops messages with no or invalid options or an invalid signature.
ipv6 nd raguard attach-policy	Applies the IPv6 RA guard feature on a specified interface.
limit address-count	Limits the number of IPv6 addresses allowed to be used on the port.
sec-level minimum	Specifies the minimum security level parameter value when CGA options are used.
trusted-port	Configures a port to become a trusted port.
validate source-mac	Checks the source MAC address against the link layer address.

ipv6 snooping policy

Note All existing IPv6 Snooping commands (prior to) now have corresponding SISF-based device-tracking commands that allow you to apply your configuration to both IPv4 and IPv6 address families.

To configure an IPv6 snooping policy and enter IPv6 snooping configuration mode, use the **ipv6 snooping policy** command in global configuration mode. To delete an IPv6 snooping policy, use the **no** form of this command.

ipv6 snooping policy *snooping-policy*
no ipv6 snooping policy *snooping-policy*

Syntax Description

snooping-policy	User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

Command Default

An IPv6 snooping policy is not configured.

Command Modes

Global configuration

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

Use the **ipv6 snooping policy** command to create an IPv6 snooping policy. When the **ipv6 snooping policy** command is enabled, the configuration mode changes to IPv6 snooping configuration mode. In this mode, the administrator can configure the following IPv6 first-hop security commands:

- The **device-role** command specifies the role of the device attached to the port.
- The **limit address-count** *maximum* command limits the number of IPv6 addresses allowed to be used on the port.
- The **protocol** command specifies that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP).
- The **security-level** command specifies the level of security enforced.
- The **tracking** command overrides the default tracking policy on a port.
- The **trusted-port** command configures a port to become a trusted port; that is, limited or no verification is performed when messages are received.

This example shows how to configure an IPv6 snooping policy:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)#
```

ipv6 traffic-filter

This command enables IPv6 traffic filter.

To enable the filtering of IPv6 traffic on an interface, use the **ipv6 traffic-filter** command. To disable the filtering of IPv6 traffic on an interface, use the **no** form of the command.

Use the **ipv6 traffic-filter** interface configuration command on the switch stack or on a standalone switch to filter IPv6 traffic on an interface. The type and direction of traffic that you can filter depends on the feature set running on the switch stack. Use the **no** form of this command to disable the filtering of IPv6 traffic on an interface.

ipv6 traffic-filter [**web**] *acl-name*
no ipv6 traffic-filter [**web**]

Syntax Description

web	(Optional) Specifies an IPv6 access name for the WLAN Web ACL.
acl-name	Specifies an IPv6 access name.

Command Default

Filtering of IPv6 traffic on an interface is not configured.

Command Modes

wlan

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6 {default | vlan}** global configuration command and reload the switch.

You can use the **ipv6 traffic-filter** command on physical interfaces (Layer 2 or Layer 3 ports), Layer 3 port channels, or switch virtual interfaces (SVIs).

You can apply an ACL to outbound or inbound traffic on Layer 3 interfaces (port ACLs), or to inbound traffic on Layer 2 interfaces (router ACLs).

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.

This example shows how to filter IPv6 traffic on an interface:

```
Device(config-wlan)# ipv6 traffic-filter TestDocTrafficFilter
```

key chain

To create or modify a keychain, use the **key chain** command. To disable this feature, use the **no** form of this command.

key chain*key-chain name* { **macsec** | **tcp** }
no key chain*key-chain name* { **macsec** | **tcp** }

Syntax Description

key-chain name	Specifies the name of the key chain.
macsec	Specifies a MacSEC key chain.
tcp	Specifies the tcp key chain.

Command Default

No default.

Command Modes

Global configuration mode.

Examples

The following example shows how to specify a key chain to identify authentication on a key-chain:

```
Device(config)# key chain key-chain-name macsec
```

Related Commands

Command	Description
key config-key	Sets a private configuration key for general use.
show key chain	Displays authentication key information.

key config-key

To set a private configuration key for private use, use the **key config-key** command. To disable this feature, use the **no** form of this command.

key config-key { **1 LINE** | **newpass** *config-key* | **password-encrypt LINE** }
no key config-key { **1 LINE** | **newpass** *config-key* | **password-encrypt LINE** }

Syntax Description

1	Sets a private configuration key for private use.
newpass	Specifies a new password without space or tabs.
config-key	Specifies the config key, with a minimum of 8 characters, and not beginning with the IOS special characters - !, #, and ;.
password-encrypt	Sets a private configuration key for password encryption.

Command Default

None

Command Modes

Global configuration mode.

Examples

The following example shows how to specify a config-key:

```
Device(config)# key config-key password-encrypt config-key
```

key config-key password-encrypt

To set a private configuration key for password encryption, use the **key config-key password-encrypt** command. To disable this feature, use the **no** form of this command.

key config-key password-encrypt <*config-key*>

Syntax Description

config-key	Enter a value with minimum 8 characters. **Note** The value must not begin with the following special characters: !, #, and ;

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 17.6.1	This command was introduced.

Examples

The following example shows how to set a username and password for AP management:

```
Device# enable
Device# configure terminal
Device(config)# key config-key password-encryption 12345678
Device(config-ap-profile)# password encryption aes
Device(config-ap-profile)# end
```

license air level

To configure AIR licenses on a wireless controller, enter the **license air level** command in global configuration mode. To revert to the default setting, use the **no** form of this command.

license air level { **air-network-advantage** [**addon air-dna-advantage**] | **air-network-essentials** [**addon air-dna-essentials**] }

no license air level

Syntax Description

air-network-advantage	Configures the AIR Network Advantage license level.
addon air-dna-advantage	(Optional) Configures the add-on AIR DNA Advantage license level. This add-on option is available with the AIR Network Advantage license.
air-network-essentials	Configures the AIR Network Essentials license level.
addon air-dna-essentials	(Optional) Configures the add-on AIR DNA Essentials license level. This add-on option is available with the AIR Network Essential license.

Command Default

For all Cisco Catalyst 9800 Wireless controllers the default license is AIR DNA Advantage.

For EWC-APs:

- Prior to Cisco IOS XE Bengaluru 17.4.1, the default license is AIR DNA Essentials.
- Starting with Cisco IOS XE Bengaluru 17.4.1, the default license is AIR Network Essentials

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	This command continues to be available and applicable with the introduction of Smart Licensing Using Policy.
Cisco IOS XE Bengaluru 17.4.1	Only for EWC-APs, the default license was changed from AIR DNA Essentials to AIR Network Essentials.

Usage Guidelines

In the Smart Licensing Using Policy environment, you can use the **license air level** command to change the license level being used on the product instance, or to additionally configure an add-on license on the product instance. The change is effective after a reload.

The licenses that can be configured are:

- AIR Network Essential
- AIR Network Advantage
- AIR DNA Essential

- AIR DNA Advantage

You can configure AIR DNA Essential or AIR DNA Advantage license level and on term expiry, you can move to the Network Advantage or Network Essentials license level, if you do not want to renew the DNA license.

Every connecting AP requires a Cisco DNA Center License to leverage the unique value properties of the controller.

Examples

The following example show how to configure the AIR DNA Essential license level:

```
Device# configure terminal
Device(config)# license air level network-essentials addon air-dna-essentials
```

The following example shows how the AIR DNA Advantage license level is configured to begin with and then changed to AIR DNA Essentials:

Current configuration as AIR DNA Advantage:

```
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Advantage

Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>
```

Configuration of AIR DNA Essentials :

```
Device# configure terminal
Device(config)# license air level air-network-essentials addon air-dna-essentials

Device# exit
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Essentials
Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>

Device# write memory
Device# reload
```

After reload:

```
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Essentials
Next reload AIR license Level: AIR DNA Essentials

Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>
```

license smart (global config)

To configure licensing-related settings such as the mode of transport and the URL that the product instance uses to communicate with Cisco Smart Software Manager (CSSM), or Cisco Smart Licensing Utility (CSLU), or Smart Software Manager On-Prem (SSM On-Prem), to configure the usage reporting interval, to configure the information that must be exluded or included in a license usage report (RUM report), enter the **license smart** command in global configuration mode. Use the **no** form of the command to revert to default values.

license smart { **custom_id** *ID* | **enable** | **privacy** { **all** | **hostname** | **version** } | **proxy** { **address** *address_hostname* | **port** *port* } | **reservation** | **server-identity-check** | **transport** { **automatic** | **callhome** | **cslu** | **off** | **smart** } | **url** { *url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* } | **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } | **utility** [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }] }

no license smart { **custom_id** | **enable** | **privacy** { **all** | **hostname** | **version** } | **proxy** { **address** *address_hostname* | **port** *port* } | **reservation** | **server-identity-check** | **transport** | **url** { *url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* } | **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } | **utility** [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }] }

Syntax Description

custom_id *ID*	Although available on the CLI, this option is not supported.
enable	Although visible on the CLI, configuring this keyword has no effect. Smart licensing is always enabled.
privacy { **all**	**hostname**	**version** }	Enables you to *leave out* certain information from the usage reports that are send to CSSM. Choose from the following options: • **all**: Sends only the minimal licensing information in any communication. • **hostname**: Excludes the hostname from any communication. • **version**: Excludes the product instance agent version from any communication.

proxy { **address** *address_hostname* | **port** *port* }	Configures a proxy for license usage synchronization with CSLU or CSSM. This means that you can use this option to configure a proxy only if the transport mode is **license smart transport smart** (CSSM), or **license smart transport cslu** (CSLU). However, you cannot configure a proxy for license usage synchronization in an SSM On-Prem deployment, which also uses **license smart transport cslu** as the transport mode. Configure the following options: • **address** *address_hostname*: Configures the proxy address. For *address_hostname*, enter the enter the IP address or hostname of the proxy. • **port***port*: Configures the proxy port. For *port*, enter the proxy port number.
reservation	Enables or disables a license reservation feature. **Note** Although available on the CLI, this option is not applicable because license *reservation* is not applicable in the Smart Licensing Using Policy environment.
server-identity-check	Enables or disables the HTTP secure server identity check.
transport { **automatic** | **callhome** | **cslu** | **off** | **smart** }	Configures the mode of transport the product instance uses to communicate with CSSM. Choose from the following options: • **automatic**: Sets the transport mode **cslu**. **Note** The **automatic** keyword is not supported on Cisco Catalyst Wireless Controllers. • **callhome**: Enables Call Home as the transport mode. • **cslu**: Enables CSLU as the transport mode. This is the default transport mode. The same keyword applies to both CSLU *and* SSM On-Prem, but the URLs are different. See **cslu***cslu_or_on-prem_url* in the following row. • **off**: Disables all communication from the product instance. • **smart**: Enables Smart transport.

url { *url* | **cslu** *cslu_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* }

Sets URL that is used for the configured transport mode. Choose from the following options:

- *url*: If you have configured the transport mode as **callhome**, configure this option. Enter the CSSM URL exactly as follows:

  `https://tools.cisco.com/its/service/oddce/services/DDCEService`

  The **no license smart url** *url* command reverts to the default URL.

- **cslu** *cslu_or_on-prem_url*: If you have configured the transport mode as **cslu**, configure this option, with the URL for CSLU or SSM On-Prem, as applicable:

  - If you are using CSLU, enter the URL as follows:

    `http://<cslu_ip_or_host>:8182/cslu/v1/pi`

    For `<cslu_ip_or_host>`, enter the hostname or the IP address of the windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.

    The **no license smart url cslu** *cslu_or_on-prem_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`

  - If you are using SSM On-Prem, enter the URL as follows:

    `http://<ip>/cslu/v1/pi/<tenant ID>`

    For <ip>, enter the hostname or the IP address of the server where you have installed SSM On-Prem. The <tenantID> must be the default local virtual account ID.

    Tip You can retrieve the entire URL from SSM On-Prem. In the software configuration guide (17.3.x and later), see Smart Licensing Using Policy > Task Library for Smart Licensing Using Policy > Retrieving the Transport URL (SSM On-Prem UI).

    The **no license smart url cslu** *cslu_or_on-prem_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`

- **default**: Depends on the configured transport mode. Only the **smart** and **cslu** transport modes are supported with this option.

  If the transport mode is set to **cslu**, and you configure **license smart url default**, the CSLU URL is configured automatically

(`https://cslu-local:8182/cslu/v1/pi`).

If the transport mode is set to **smart**, and you configure **license smart url default**, the Smart URL is configured automatically (`https://smartreceiver.cisco.com/licservice/license`).

- **smart** *smart_url*: If you have configured the transport type as **smart**, configure this option. Enter the URL exactly as follows:

  `https://smartreceiver.cisco.com/licservice/license`

  When you configure this option, the system automatically creates a duplicate of the URL in **license smart url** *url*. You can ignore the duplicate entry, no further action is required.

  The **no license smart url smart***smart_url* command reverts to the default URL.

- **utility** *smart_url*: Although available on the CLI, this option is not supported.

usage { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* }	Configures usage reporting settings. You can set the following options: • **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value*: Defines strings for inclusion in data models, for telemetry. Up to 4 strings (or tags) may be defined. For *tag_value*, enter the string value for each tag that you define. • **interval** *interval_in_days*: Sets the reporting interval in days. By default the RUM report is sent every 30 days. The valid value range is 1 to 3650. If you set the value to zero, RUM reports are not sent, regardless of what the applied policy specifies - this applies to topologies where CSLU or CSSM may be on the receiving end. If you set a value that is greater than zero and the transport type is set to **off**, then, between the *interval_in_days* and the policy value for `Ongoing reporting frequency(days):`, the lower of the two values is applied. For example, if *interval_in_days* is set to 100, and the value in the in the policy says `Ongoing reporting frequency (days):90`, RUM reports are sent every 90 days. If you do not set an interval, and the default is effective, the reporting interval is determined entirely by the policy value. For example, if the default value is effective and only unenforced licenses are in use, if the policy states that reporting is not required, then RUM reports are not sent.
utility [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }]	Although visible on the CLI, this option is not supported.

Command Default

Cisco IOS XE Amsterdam 17.3.1 or earlier: Smart Licensing is enabled by default.

Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy is enabled by default.

Command Modes

Global config (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	The following keywords and variables were introduced with Smart Licensing Using Policy: • Under the **url**keyword, these options were introduced: { **cslu** *cslu_url* | **smart** *smart_url* } • Under the **transport** keyword, these options were introduced: { **cslu** | **off** } Further, the default transport type was changed from **callhome**, to **cslu**. • **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } The following keywords and variables under the **license smart** command are deprecated and no longer available on the CLI: **enable**and **conversion automatic**.
Cisco IOS XE Amsterdam 17.3.3	SSM On-Prem support was introduced. For product instance-initiated communication in an SSM On-Prem deployment, the existing [**no**]**license smart url cslu***cslu_or_on-prem_url* command supports the configuration of a URL for SSM On-Prem as well. But the required URL format for SSM On-Prem is: `http://<ip>/cslu/v1/pi/<tenant ID>`. The corresponding transport mode that must be configured is also an existing command (**license smart transport cslu**).

Usage Guidelines

The reporting interval that you configure (**license smart usage interval** *interval_in_days* command), determines the date and time at which the product instance sends out the RUM report. If the scheduled interval coincides with a communication failure, the product instance attempts to send out the RUM report for up to four hours after the scheduled time has expired. If it is still unable to send out the report (because the communication failure persists), the system resets the interval to 15 minutes. Once the communication failure is resolved, the system reverts the reporting interval to the value that you last configured.

The system message you may see in case of a communicatin failure is %SMART_LIC-3-COMM_FAILED. For information about resolving this error and restoring the reporting interval value, in the software configuration guide of the required release (17.3.x onwards), see *System Configuration* > *Smart Licensing Using Policy* > *Troubleshooting Smart Licensing Using Policy*.

Examples

- Examples for Data Privacy, on page 327
- Examples for Transport Type and URL, on page 327
- Examples for Usage Reporting Options, on page 328

Examples for Data Privacy

The following examples show how to configure data privacy related information using **license smart privacy** command in global configuration mode. The accompanying **show license status** output displays configured information.

No private information is sent:

```
Device# configure terminal
Device(config)# license smart privacy all
Device(config)# license smart transport callhome
Device(config)# license smart url
https://tools.cisco.com/its/service/oddce/services/DDCEService
Device(config)# exit
Device# show license status
<output truncated>
Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: ENABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: ENABLED

Transport:
  Type: Callhome
<output truncated>
```

Agent version on the product instance is not sent:

```
Device# configure terminal
Device(config)# license smart privacy version
Device(config)# license smart transport callhome
Device(config)# license smart url
https://tools.cisco.com/its/service/oddce/services/DDCEService
Device(config)# exit
Device# show license status
<output truncated>
Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: ENABLED

Transport:
  Type: Callhome
<output truncated>
```

Examples for Transport Type and URL

The following examples show how to configure some of the transport types using the **license smart transport** and the **license smart url** commands in global configuration mode. The accompanying **show license all** output displays configured information.

Transport **cslu**:

```
Device# configure terminal
Device(config)# license smart transport cslu
Device(config)# license smart url default
Device(config)# exit
Device# show license all
<output truncated>
```

```
Transport:
  Type: cslu
  Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  Proxy:
    Not Configured
<output truncated>
```

Transport **smart**:

```
Device# configure terminal
Device(config)# license smart transport smart
Device(config)# license smart url smart https://smartreceiver.cisco.com/licservice/license
Device(config)# exit
Device# show license all
<output truncated>
Transport:
  Type: Smart
  URL: https://smartreceiver-stage.cisco.com/licservice/license
  Proxy:
    Not Configured
<output truncated>
```

Examples for Usage Reporting Options

The following examples show how to configure some of the usage reporting settings using the **license smart usage** command in global configuration mode. The accompanying **show running-config** output displays configured information.

Configuring the **customer-tag** option:

```
Device# configure terminal
Device(config)# license smart usage customer-tags tag1 SA/VA:01
Device(config)# exit
Device# show running-config | include tag1
license smart usage customer-tags tag1 SA/VA:01
```

Configuring a narrower reporting interval than the currently applied policy:

```
Device# show license status
<output truncated>
Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Dec 21 12:02:21 2020 PST
Reporting push interval: 30 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 22 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>

Device# configure terminal
Device(config)# license smart usage interval 20
Device(config)# exit
Device# show license status
<output truncated>

Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Nov 22 12:02:21 2020 PST
Reporting push interval: 20 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 12 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
```

```
Last report file write: <none>
<output truncated>
```

license smart (privileged EXEC)

To configure licensing functions such as requesting or returning authorization codes, saving Resource Utilization Measurement reports (RUM reports), importing a file on to a product instance, establishing trust with Cisco Smart Software Manager (CSSM), synchronizing the product instance with CSSM, or Cisco Smart License Utility (CSLU), or Smart Software Manager On-Prem (SSM On-Prem), and removing licensing information from the product instance, enter the **license smart** command in privileged EXEC mode with the corresponding keyword or argument.

license smart { **authorization** { **request** { **add** | **replace** } *feature_name* { **all** | **local** } | **return** { **all** | **local** } { **offline** [*path*] | **online** } } | **clear eventlog** | **export return** { **all** | **local** } *feature_name* | **factory reset** | **import** *file_path* | **save** { **trust-request** *filepath_filename* | **usage** { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *file_path* } } | **sync** { **all** | **local** } | **trust idtoken** *id_token_value* { **local** | **all** } [{ **force** }] }

Syntax Description

smart	Provides options for Smart Licensing.
authorization	Provides the option to request for, or return, authorization codes. Authorization codes are required *only* if you use licenses with enforcement type: export-controlled or enfored.
request	Requests an authorization code from CSSM, CSLU (CSLU in-turn fetches it from CSSM), or SSM On-Prem and installs it on the product instance.
add	Adds the requested license to the existing authorization code. The new authorization code will contain all the licenses of the existing authorization code and the requested license.
replace	Replaces the existing authorization code. The new authorization code will contain only the requested license. All licenses in the current authorization code are returned. When you enter this option, the product instance verifies if licenses that correspond to the authorization codes that will be removed, are in-use. If licenses are being used, an error message tells you to first disable the corresponding features.
feature_name	Name of the license for which you are requesting an authorization code.
all	Performs the action for all product instances in a High Availability configuration.
local	Performs the action for the *active* product instance. This is the default option.
return	Returns an authorization code back to the license pool in CSSM.
offline *file_path*	Means the product instance is not connected to CSSM. The authorization code is returned offline. This option requires you to print the return code to a file. Optionally, you can also specify a path to save the file. The file format can be any readable format, such as `.txt` If you choose the offline option, you must complete the additional step of copying the return code from the CLI or the saved file and entering it in CSSM.

online	Means that the product instance is in a connected mode. The authorization code is returned to CSLU or CSSM directly.
clear eventlog	Clears all event log files from the product instance.
export return	Returns the authorization key for an export-controlled license.
factory reset	Clears all saved licensing information from the product instance.
import *filepath_filename*	Imports a file on to the product instance. The file may be that of an authorization code, a trust code, or, or a policy. For *filepath_filename*, specify the location, including the filename.
save	Provides options to save RUM reports or trust code requests.
trust-request *filepath_filename*	Saves the trust code request for the active product instance in the specified location. For *filepath_filename*, specify the absolute path to the file, including the filename.
usage { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *file_path* }	Saves RUM reports (license usage information) in the specified location. You must specify one of these options: • **all**: Saves all RUM reports. • **days** *days*: Saves RUM report for the last *n* number of days (excluding the current day). Enter a number. The valid range is 0 to 4294967295. For example, if you enter 3, RUM reports of the last three days are saved. • **rum-Id** *rum-ID*: Saves a specified RUM ID. The valid value range is 0 to 18446744073709551615. • **unreported**: Saves all unreported RUM reports. **file** *filepath_filename*: Saves the specified usage information to a file. Specify the absolute path to the file, including the filename.
sync { **all** | **local** }	Synchronizes with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data. This includes uploading pending RUM reports, downloading the ACK response, any pending authorization codes, trust codes, and policies for the product instance. Specify the product instance by entering one of these options: • **all**: Performs synchronization for all the product instances in a High Availability set-up. If you choose this option, the product instance also sends the list of all the UDIs in the synchronization request. • **local**: Performs synchronization only for the active product instance sending the request, that is, its own UDI. This is the default option.
trust idtoken *id_token_value*	Establishes a trusted connection with CSSM. To use this option, you must first generate a token in the CSSM portal. Provide the generated token value for *id_token_value*.

force	Submits a trust code request even if a trust code already exists on the product instance. A trust code is node-locked to the UDI of a product instance. If the UDI is already registered, CSSM does not allow a new registration for the same UDI. Entering the **force** keyword overrides this behavior.

Command Default

Cisco IOS XE Amsterdam 17.3.1 or earlier: Smart Licensing is enabled by default.

Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy is enabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	The following keywords and variables were introduced with Smart Licensing Using Policy: • **authorization** { **request** { **add** | **replace** } *feature_name* { **all** | **local** } | **return** { **all** | **local** } { **offline** [*path*] | **online** } } • **import** *file_path* • **save** { **trust-request** *filepath_filename* | **usage** { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *file_path* } } • **sync** { **all** | **local** } • **trust idtoken** *id_token_value* { **local** | **all** } [**force**] The following keywords and variables under the **license smart** command are deprecated and no longer available on the CLI: • **register idtoken** *token_id* [**force**] • **renew id** { **ID** | **auth** } • **debug** { **error** | **debug** | **trace** | **all** } • **reservation** { **cancel** [**all** | **local**] | **install** [**file**] *key* | **request** { **all** | **local** | **universal** } | **return** [**all** | **authorization** { *auth_code* | **file** *filename* } | **Local**] *key* } • **mfg reservation** { **request** | **install** | **install file** | **cancel** } • **conversion** { **start** | **stop** }
Cisco IOS XE Amsterdam 17.3.3	Support for SSM On-Prem was introduced. You can perform licensing-related tasks such as saving Resource Utilization Measurement reports (RUM reports), importing a file on to a product instance, synchronizing the product instance, returning authorization codes, and removing licensing information from the product instance in an SSM On-Prem deployment.

Usage Guidelines

Overwriting a Trust Code

Use case for the **force** option when configuring the **license smart trust idtoken** command: You use same token for all the product instances that are part of one Virtual Account. If the product instance has moved from one account to another (for instance, because it was added to a High Availability set-up, which is part of another Virtual Account), then there may be an existing trust code you have to overwrite.

Removing Licensing Information

Entering the **licence smart factory reset** command removes all licensing information (except the licenses in-use) from the product instance, including any authorization codes, RUM reports etc. Therefore, we recommend the use of this command only if the product instance is being returned (Return Material Authrization, or RMA), or being decommissioned permanently. We also recommend that you send a RUM report to CSSM, before you remove licensing information from the product instance - this is to ensure that CSSM has up-to-date usage information.

Authorization Codes and License Reservations:

Options relating to authorization codes and license reservations:

- Since there are no export-controlled or enforced licenses on any of the Cisco Catalyst Wireless Controllers, and the notion of reserved licenses is not applicable in the Smart Licensing Using Policy environment, the following commands are not applicable:
  - **license smart authorization request** { **add** | **replace** } *feature_name* { **all** | **local** }
  - **license smart export return**
- The following option is applicable and required for any SLR authorization codes you may want to return:

  license smart authorization return { **all** | **local** } { **offline** [*path*] | **online** }

Examples

- Example for Saving Licensing Usage Information, on page 333
- Example for Installing a Trust Code, on page 334
- Example for Returning an SLR Authorization Code, on page 334

Example for Saving Licensing Usage Information

The following example shows how you can save license usage information on the product instance. You can use this option to fulfil reporting requirements in an air-gapped network. In the example, the file is first save to flash memory and then copied to a TFTP location:

```
 Device> enable
Device# license smart save usage unreported file flash:RUM-unrep.txt
Device# dir
Directory of bootflash:/

33      -rw-             5994   Nov 2 2020 03:58:04 +05:00  RUM-unrep.txt

Device# copy flash:RUM-unrep.txt tftp://192.168.0.1//auto/tftp-user/user01/
Address or name of remote host [192.168.0.1]?
Destination filename [//auto/tftp-user/user01/RUM-unrep.txt]?
```

```
!!
15128 bytes copied in 0.161 secs (93963 bytes/sec)
```

After you save RUM reports to a file, you must upload it to CSSM (from a workstation that has connectivity to the internet, and Cisco).

Example for Installing a Trust Code

The following example shows how to install a trust code even if one is already installed on the product instance. This requires connectivity to CSSM. The accompanying **show license status** output shows sample output after successful installation:

Before you can install a trust code, you must generate a token and download the corresponding file from CSSM.

Use the **show license status** command (`Trust Code Installed:`) to verify results.

```
Device> enable
Device# license smart trust idtoken
NGMwMjk5mYtNZaxMS00NzMZmtgWm local force

Device# show license status
<output truncated>
Trust Code Installed:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
    INSTALLED on Nov 02 05:19:05 2020 IST
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
    INSTALLED on Nov 02 05:19:05 2020 IST
<output truncated>
```

Example for Returning an SLR Authorization Code

The following example shows how to remove and return an SLR authorization code. Here the code is returned offline (no connectivity to CSSM). The accompanying **show license all** output shows sample output after successful return:

```
Device> enable
Device# show license all
<output truncated>
License Authorizations
======================
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
      Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      Last Confirmation code: ad4382fe
<output truncated>

Device# license smart authorization return local offlline
Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS
    Return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h
UDI: PID:C9800-CL-K9,SN:9XECPSUU4XN
    Return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA

Device# show license all
<output truncated>
```

```
License Authorizations
======================
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: NOT INSTALLED
      Last return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: NOT INSTALLED
      Last return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA
<output truncated>
```

If you choose the **offline** option, you must complete the additional step of copying the return code from the CLI or the saved file and entering it in CSSM.

local-auth ap eap-fast

To configure Flex policy local authentication using EAP Fast method, use the **local-auth ap eap-fast** command.

local-auth ap eap-fast *profile-name*

Syntax Description

profile-name	Enter eap-fast profile name.

Command Default None

Command Modes config-wireless-flex-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure EAP Fast method authentication on a Flex policy:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile flex profile-name
Device(config-wireless-flex-profile)# local-auth ap eap-fast eap-fast-profile-name
```

local-site

To configure the site as local site, use the **local-site** command.

local-site

Syntax Description

local-site	Configure this site as local site.

Command Default

None

Command Modes

config-site-tag

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to set the current site as local site:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless tag site tag-name
Device(config-site-tag)# local-site
```

location expiry

To configure the location expiry duration, use the **location expiry** command in global configuration mode.

location expiry {**calibrating-client** | **client** | **tags** }*timeout-duration*

Syntax Description

calibrating-client	Timeout value for calibrating clients.
client	Timeout value for clients.
tags	Timeout value for RFID tags.
timeout-duration	Timeout duration, in seconds.

Command Default

Timeout value is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to configure the location expiry duration:

```
Device(config)# location expiry tags 50
```

location notify-threshold

To configure the NMSP notification threshold for RSSI measurements, use the **location notify-threshold** command in global configuration mode. To remove the NMSP notification threshold for RSSI measurements, use the **no** form of this command.

location notify-threshold {**client** | **rogue-aps** | **tags** } *db*
no location notify-threshold {**client** | **rogue-aps** | **tags** }

Syntax Description

client	Specifies the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
rogue-aps	Specifies the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
tags	Specifies the NMSP notification threshold (in dB) for RFID tags. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
db	The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure the NMSP notification threshold to 10 dB for clients. A notification NMSP message is sent to MSE as soon as the client RSSI changes by 10 dB:

```
Device# configure terminal
Device(config)# location notify-threshold client 10
Device(config)# end
```

log-export-mode

To configure the log export using FTP, STP and TFTP, use the **log-export-mode** command. Use the **no** command to negate the command or to set the command to its default.

log-export-mode { **ftp** | **stp** | **tftp** }

no log-export-mode { **ftp** | **stp** | **tftp** }

Syntax Description

ftp	Configures the log export using FTP.
stp	Configures the log export using STP.
tftp	Configures the log export using TFTP.

Command Default

None

Command Modes

Wireless trace export profile configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile transfer trace-export trace-export-name
Device(config-wireless-trace-export-profile)# log-export-mode tftp
```

mab request format attribute

To configure the delimiter while configuring MAC filtering on a WLAN, use the mab request format attribute command.

mab request format attribute *username password nas-identifier]*

Syntax Description

username	Username format used for MAB requests
password	Global Password used for all MAB requests
Nas-identifier	NAS-Identifier attribute

Command Default

Global Configuration

Command Modes

MAC is sent without any delimiter.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

MAC is sent without any delimiter.

Example

The following example shows how to configure delimiter while configuring MAC filtering:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# mab request format attribute 1 groupsize 4
```

mac-filtering

To enable MAC filtering on a WLAN, use the **mac-filtering** command.

mac-filtering [*mac-authorization-list*]

Syntax Description

mac-authorization-list	Name of the Authorization list.

Command Default

None

Command Modes

config-wlan

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to enable MAC filtering on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan-name wlan-index SSID-name
Device(config-wlan)# mac-filtering
```

match activated-service-template

To create a condition that evaluates true based on the service template activated on a session, use the **match activated-service-template** command in control class-map filter configuration mode. To create a condition that evaluates true if the service template activated on a session does not match the specified template, use the **no-match activated-service-template** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match activated-service-template *template-name*
no-match activated-service-template *template-name*
no {**match** | **no-match**} **activated-service-template** *template-name*

Syntax Description

template-name	Name of a configured service template as defined by the **service-template** command.

Command Default

The control class does not contain a condition based on the service template.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **match activated-service-template** command configures a match condition in a control class based on the service template applied to a session. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true for the actions of the control policy to be executed.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match activated-service-template SVC_1** command, all template values except SVC_1 are accepted as a successful match.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class that evaluates true if the service template named VLAN_1 is activated on the session:

```
class-map type control subscriber match-all CLASS_1
 match activated-service-template VLAN_1
```

Related Commands

Command	Description
activate (policy-map action)	Activates a control policy or service template on a subscriber session.
class	Associates a control class with one or more actions in a control policy.
match service-template	Creates a condition that evaluates true based on an event's service template.

Command	Description
service-template	Defines a template that contains a set of service policy attributes to apply to subscriber sessions.

match any

To perform a match on any protocol that passes through the device, use the **match any** command.

match any

Command Default None

Command Modes config-cmap

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to match any packet passing through the device:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map cmap-name
Device(config-cmap)# match any
```

match message-type

To set a message type to match a service list, use the **match message-type** command.

match message-type {**announcement** | **any** | **query**}

Syntax Description

announcement	Allows only service advertisements or announcements for the Switch.
any	Allows any match type.
query	Allows only a query from the client for a certain Switch in the network.

Command Default

None

Command Modes

Service list configuration.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

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, with each one having a permit or deny result. The evaluation of a 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 a permit/deny action associated with the statement match is performed. The default action after scanning through the entire list is to deny.

Note It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

Example

The following example shows how to set the announcement message type to be matched:

```
Switch(config-mdns-sd-sl)# match message-type announcement
```

match non-client-nrt

To match non-client NRT (non-real-time), use the **match non-client-nrt** command in class-map configuration mode. Use the **no** form of this command to return to the default setting.

match non-client-nrt
no match non-client-nrt

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Class-map

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None

This example show how you can configure non-client NRT:

```
Device(config)# class-map test_1000
Device(config-cmap)# match non-client-nrt
```

match protocol

To configure the match criterion for a class map on the basis of a specified protocol, use the **match protocol** command in class-map configuration or policy inline configuration mode. To remove the protocol-based match criterion from the class map, use the **no** form of this command. For more information about the **match protocol** command, refer to the *Cisco IOS Quality of Service Solutions Command Reference*.

match protocol {*protocol-name* | **attribute category** *category-name* | **attribute sub-category** *sub-category-name* | **attribute application-group** *application-group-name*}

Syntax Description

protocol-name	Name of the protocol (for example, bgp) used as a matching criterion.
category-name	Name of the application category used as a matching criterion.
sub-category-name	Name of the application subcategory used as a matching criterion.
application-group-name	Name of the application group as a matching criterion. When the application name is specified, the application is configured as the match criterion instead of the application group.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to create class maps with apply match protocol filters for application name, category, and sub category:

```
Device# configure terminal
Device(config)# class-map cat-browsing
Device(config-cmap)# match protocol attribute category browsing
Device(config-cmap)#end

Device# configure terminal
Device(config)# class-map cat-fileshare
Device(config-cmap)# match protocol attribute category file-sharing
Device(config-cmap)#end

Device# configure terminal
Device(config)# class-map match-any subcat-terminal
Device(config-cmap)# match protocol attribute sub-category terminal
Device(config-cmap)#end

Device# configure terminal
Device(config)# class-map match-any webex-meeting
Device(config-cmap)# match protocol webex-meeting
Device(config-cmap)#end
```

This example shows how to create policy maps and define existing class maps for upstream QoS:

```
Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class cat-browsing
Device(config-pmap-c)# police 150000
Device(config-pmap-c)# set dscp 12
Device(config-pmap-c)#end


Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class cat-fileshare
Device(config-pmap-c)# police 1000000
Device(config-pmap-c)# set dscp 20
Device(config-pmap-c)#end


Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class subcat-terminal
Device(config-pmap-c)# police 120000
Device(config-pmap-c)# set dscp 15
Device(config-pmap-c)#end

Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class webex-meeting
Device(config-pmap-c)# police 50000000
Device(config-pmap-c)# set dscp 21
Device(config-pmap-c)#end
```

This example shows how to create policy maps and define existing class maps for downstream QoS:

```
Device# configure terminal
Device(config)# policy-map test-avc-down
Device(config-pmap)# class cat-browsing
Device(config-pmap-c)# police 200000
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)#end


Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class cat-fileshare
Device(config-pmap-c)# police 300000
Device(config-pmap-c)# set wlan user-priority 2
Device(config-pmap-c)# set dscp 20
Device(config-pmap-c)#end


Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class subcat-terminal
Device(config-pmap-c)# police 100000
Device(config-pmap-c)# set dscp 25
Device(config-pmap-c)#end

Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class webex-meeting
Device(config-pmap-c)# police 60000000
```

```
Device(config-pmap-c)# set dscp 41
Device(config-pmap-c)#end
```

This example shows how to apply defined QoS policy on a WLAN:

```
Device# configure terminal
Device(config)#wlan  alpha
Device(config-wlan)#shut
Device(config-wlan)#end
Device(config-wlan)#service-policy client input test-avc-up
Device(config-wlan)#service-policy client output test-avc-down
Device(config-wlan)#no shut
Device(config-wlan)#end
```

match service-instance

To set a service instance to match a service list, use the **match service-instance** command.

match service-instance *line*

Syntax Description

line	Regular expression to match the service instance in packets.

Command Default

None

Command Modes

Service list configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

Example

The following example shows how to set the service instance to match:

```
Switch(config-mdns-sd-sl)# match service-instance servInst 1
```

match service-type

To set the value of the mDNS service type string to match, use the **match service-type** command.

match service-type *line*

Syntax Description

line	Regular expression to match the service type in packets.

Command Default

None

Command Modes

Service list configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

Example

The following example shows how to set the value of the mDNS service type string to match:

```
Switch(config-mdns-sd-sl)# match service-type _ipp._tcp
```

match user-role

To configure the class-map attribute filter criteria, use the **match user-role** command.

match user-role *user-role*

Command Default None

Command Modes config-filter-control-classmap

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure a class-map attribute filter criteria:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map type control subscriber match-any map-name
Device(config-filter-control-classmap)# match user-role user-role
```

match username

To create a condition that evaluates true based on an event's username, use the **match username** command in control class-map filter configuration mode. To create a condition that evaluates true if an event's username does not match the specified username, use the **no-match username** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match username *username*
no-match username *username*
no {**match** | **no-match**} **username** *username*

Syntax Description

username	Username.

Command Default

The control class does not contain a condition based on the event's username.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

The **match username** command configures a match condition in a control class based on the username. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match username josmithe** command, the control class accepts any username value except josmithe as a successful match.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class that evaluates true if the username is josmithe:

```
class-map type control subscriber match-all CLASS_1
 match username josmithe
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
policy-map type control subscriber	Defines a control policy for subscriber sessions

match (access-map configuration)

To set the VLAN map to match packets against one or more access lists, use the **match** command in access-map configuration mode. Use the **no** form of this command to remove the match parameters.

{**match ip address** {*namenumber*} [{*namenumber*}] [{*namenumber*}]**...** | **mac address** *name* [*name*] [*name*]**...**}
{**no match ip address** {*namenumber*} [{*namenumber*}] [{*namenumber*}]**...** | **mac address** *name* [*name*] [*name*]**...**}

Syntax Description

ip address	Set the access map to match packets against an IP address access list.
mac address	Set the access map to match packets against a MAC address access list.
name	Name of the access list to match packets against.
number	Number of the access list to match packets against. This option is not valid for MAC access lists.

Command Default

The default action is to have no match parameters applied to a VLAN map.

Command Modes

Access-map configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.

In access-map configuration mode, use the **match** command to define the match conditions for a VLAN map applied to a VLAN. Use the **action** command to set the action that occurs when the packet matches the conditions.

Packets are matched only against access lists of the same protocol type; IP packets are matched against IP access lists, and all other packets are matched against MAC access lists.

Both IP and MAC addresses can be specified for the same map entry.

Examples

This example shows how to define and apply a VLAN access map *vmap4* to VLANs 5 and 6 that will cause the interface to drop an IP packet if the packet matches the conditions defined in access list *al2*.

```
Device(config)# vlan access-map vmap4
Device(config-access-map)# match ip address al2
Device(config-access-map)# action drop
Device(config-access-map)# exit
```

```
Device(config)# vlan filter vmap4 vlan-list 5-6
```

You can verify your settings by entering the **show vlan access-map** privileged EXEC command.

match (class-map configuration)

To define the match criteria to classify traffic, use the **match** command in class-map configuration mode. Use the **no** form of this command to remove the match criteria.

Cisco IOS XE Everest 16.5.x and Earlier Releases

match {**access-group**{**name***acl-name acl-index*} | **class-map** *class-map-name* | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **precedence** *precedence-value1...value4* | **qos-group** *qos-group-value* | **vlan** *vlan-id*}
no match {**access-group**{**name***acl-name acl-index*} | **class-map** *class-map-name* | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **precedence** *precedence-value1...value4* | **qos-group** *qos-group-value* | **vlan** *vlan-id*}

Cisco IOS XE Everest 16.6.x and Later Releases

match {**access-group**{**name** *acl-name acl-index*} | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **mpls** *experimental-value* | **non-client-nrt** | **precedence** *precedence-value1...value4* | **protocol** *protocol-name* | **qos-group** *qos-group-value* | **vlan** *vlan-id* | **wlan** *wlan-id*}
no match {**access-group**{**name** *acl-name acl-index*} | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **mpls** *experimental-value* | **non-client-nrt** | **precedence** *precedence-value1...value4* | **protocol** *protocol-name* | **qos-group** *qos-group-value* | **vlan** *vlan-id* | **wlan** *wlan-id*}

Syntax Description

access-group	Specifies an access group.
name *acl-name*	Specifies the name of an IP standard or extended access control list (ACL) or MAC ACL.
acl-index	Specifies the number of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699.
class-map *class-map-name*	Uses a traffic class as a classification policy and specifies a traffic class name to use as the match criterion.
cos *cos-value*	Matches a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking. The cos-value is from 0 to 7. You can specify up to four CoS values in one **match cos** statement, separated by a space.
dscp *dscp-value*	Specifies the parameters for each DSCP value. You can specify a value in the range 0 to 63 specifying the differentiated services code point value.

ip dscp *dscp-list*	Specifies a list of up to eight IP Differentiated Services Code Point (DSCP) values to match against incoming packets. Separate each value with a space. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value.
ip precedence *ip-precedence-list*	Specifies a list of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
precedence *precedence-value1...value4*	Assigns an IP precedence value to the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
qos-group *qos-group-value*	Identifies a specific QoS group value as a match criterion. The range is 0 to 31.
vlan *vlan-id*	Identifies a specific VLAN as a match criterion. The range is 1 to 4094.
mpls *experimental-value*	Specifies Multi Protocol Label Switching specific values.
non-client-nrt	Matches a non-client NRT (non-real-time).
protocol *protocol-name*	Specifies the type of protocol.
wlan *wlan-id*	Identifies 802.11 specific values.

Command Default

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

The **match** command is used to specify which fields in the incoming packets are examined to classify the packets. Only the IP access group or the MAC access group matching to the Ether Type/Len are supported.

If you enter the **class-map match-any***class-map-name* global configuration command, you can enter the following **match** commands:

- **match access-group name** *acl-name*

Note The ACL must be an extended named ACL.

- **match ip dscp** *dscp-list*
- **match ip precedence** *ip-precedence-list*

The **match access-group** *acl-index* command is not supported.

To define packet classification on a physical-port basis, only one **match** command per class map is supported. In this situation, the **match-any** keyword is equivalent.

For the **match ip dscp** *dscp-list* or the **match ip precedence** *ip-precedence-list* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **match ip dscp af11** command, which is the same as entering the **match ip dscp 10** command. You can enter the **match ip precedence critical** command, which is the same as entering the **match ip precedence 5** command. For a list of supported mnemonics, enter the **match ip dscp ?** or the **match ip precedence ?** command to see the command-line help strings.

Use the **input-interface** *interface-id-list* keyword when you are configuring an interface-level class map in a hierarchical policy map. For the *interface-id-list*, you can specify up to six entries.

Examples

This example shows how to create a class map called class2, which matches all the incoming traffic with DSCP values of 10, 11, and 12:

```
Device(config)# class-map class2
Device(config-cmap)# match ip dscp 10 11 12
Device(config-cmap)# exit
```

This example shows how to create a class map called class3, which matches all the incoming traffic with IP-precedence values of 5, 6, and 7:

```
Device(config)# class-map class3
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# exit
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using acl1:

```
Device(config)# class-map class2
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# no match ip precedence
Device(config-cmap)# match access-group acl1
Device(config-cmap)# exit
```

This example shows how to specify a list of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

This example shows how to specify a range of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

match wlan user-priority

To match 802.11 specific values, use the **match wlan user-priority** command in class-map configuration mode. Use the **no** form of this command to return to the default setting.

match wlan user-priority *wlan-value* [*wlan-value*] [*wlan-value*] [*wlan-value*]
no match wlan user-priority *wlan-value* [*wlan-value*] [*wlan-value*] [*wlan-value*]

Syntax Description

wlan-value	The 802.11-specific values. Enter the user priority 802.11 TID user priority (0-7). (Optional) Enter up to three user priority values separated by white-spaces.

Command Default

None

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None

This example show how you can configure user-priority values:

```
Device(config)# class-map test_1000
Device(config-cmap)# match wlan user-priority 7
```

max-bandwidth

To configure the wireless media-stream's maximum expected stream bandwidth in Kbps, use the **max-bandwidth** command.

max-bandwidth *bandwidth*

Syntax Description

bandwidth	Maximum Expected Stream Bandwidth in Kbps. Valid range is 1 to 35000 Kbps.

Command Default

None

Command Modes

media-stream

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure wireless media-stream bandwidth in Kbps:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group doc-grp 224.0.0.0 224.0.0.223
Device(config-media-stream)# max-bandwidth 3500
```

max-through

To limit multicast router advertisements (RAs) per VLAN per throttle period, use the **max-through** command in IPv6 RA throttle policy configuration mode. To reset the command to its defaults, use the **no** form of this command.

max-through {*mt-value* | **inherit** | **no-limit**}

Syntax Description

mt-value	Number of multicast RAs allowed on the VLAN before throttling occurs. The range is from 0 through 256.
inherit	Merges the setting between target policies.
no-limit	Multicast RAs are not limited on the VLAN.

Command Default

10 RAs per VLAN per 10 minutes

Command Modes

IPv6 RA throttle policy configuration (config-nd-ra-throttle)

Command History

Release	Modification
Cisco IOS XE Release 3.2XE	This command was introduced.

Usage Guidelines

The **max-through** command limits the amount of multicast RAs that are passed through to the VLAN per throttle period. This command can be configured only on a VLAN.

Example

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# max-through 25
```

mdns-sd

To configure the mDNS service discovery gateway, use the **mdns-sd** command. To disable the configuration, use the **no** form of this command.

mdns-sd { **gateway** | **service-definition** *service-definition-name* | **service-list** *service-list-name* { **IN** | **OUT** } | **service-policy** *service-policy-name* }

no mdns-sd { **gateway** | **service-definition** *service-definition-name* | **service-list** *service-list-name* { **IN** | **OUT** } | **service-policy** *service-policy-name* }

Syntax Description

mdns-sd	Configures the mDNS service discovery gateway.
gateway	Configures mDNS gateway.
service-definition	Configures mDNS service definition.
service-definition-name	Specifies the mDNS service definition name.
service-list	Configures mDNS service list.
service-list-name	Specifies the mDNS service definition name.
IN	Specifies the inbound filtering.
OUT	Specifies the outbound filtering.
service-policy	Configures mDNS service policy.
service-policy-name	Specifies the mDNS service policy name.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to configure the mDNS service discovery gateway:

```
Device(config)# mdns-sd gateway
```

mdns-sd flex-profile

To configure the mDNS service discovery flex profile, use the **mdns-sd flex-profile** command. To disable the command, use the **no** form of this command.

mdns-sd flex-profile *flex-profile-name*

no mdns-sd flex-profile *flex-profile-name*

Syntax Description

mdns-sd flex-profile	Configures the mDNS service discovery flex profile.
flex-profile-name	Specifies the mDNS flex profile name.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to configure the mDNS service discovery flex profile:

```
Device(config)# mdns-sd flex-profile mdns-flex-profile
```

mdns-sd profile

To apply the mDNS flex profile to the wireless flex profile, use the **mdns-sd profile** command in the wireless flex profile mode. To disable the command, use the **no** form of this command.

mdns-sd profile *flex-profile-name*

no mdns-sd profile *flex-profile-name*

Syntax Description

mdns-sd profile	Configures the mDNS flex profile in the wireless flex profile.
flex-profile-name	Specifies the mDNS flex profile name.

Command Default

None

Command Modes

Wireless flex profile configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to apply the mDNS flex profile to the wireless flex profile:

```
Device(config-wireless-flex-profile)# mdns-sd profile mdns-flex-profile
```

method fast

To configure EAP profile to support EAP-FAST method, use the **method fast** command.

method fast [**profile** *profile-name*]

Syntax Description

profile-name	Specify the method profile.

Command Default

None

Command Modes

config-eap-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to enable EAP Fast method on a EAP profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# eap profile profile-name
Device(config-eap-profile)# method fast
```

mgmtuser username

To set a username and password for AP management, use the **mgmtuser username** command. To disable this feature, use the **no** form of this command.

mgmtuser username *username* **password {0 | 8}** *password*

Syntax Description

username	Enter a username for AP management.
0	Specifies an UNENCRYPTED password.
8	Specifies an AES encrypted password.
password	Configures the encryption password (key).

Command Default

None

Command Modes

AP Profile Configuration (config-ap-profile)

Command History

Release	Modification
Cisco IOS XE Gibraltar 17.6.1	This command was introduced.

Examples

The following example shows how to set a username and password for AP management:

```
Device# enable
Device# configure terminal
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# mgmtuser username myusername password 0
Device(config-ap-profile)# end
```

mop sysid

To enable an interface to send out periodic Maintenance Operation Protocol (MOP) system identification messages, use the **mopsysid** command in interface configuration mode. To disable MOP message support on an interface, use the **no** form of this command.

mop sysid
no mop sysid

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can still run MOP without having the background system ID messages sent. This command lets you use the MOP remote console, but does not generate messages used by the configurator.

Examples

The following example enables serial interface 0 to send MOP system identification messages:

```
Router(config)# interface serial 0
Router(config-if)# mop sysid
```

Related Commands

Command	Description
mop device-code	Identifies the type of device sending MOP sysid messages and request program messages.
mop enabled	Enables an interface to support the MOP.

nac

To enable RADIUS Network Admission Control (NAC) support for a WLAN, use the **nac** command. To disable NAC out-of-band support, use the **no** form of this command.

nac
no nac

Syntax Description

This command has no keywords or arguments.

Command Default

NAC is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

You should enable AAA override before you enable the RADIUS NAC state.

This example shows how to configure RADIUS NAC on the WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# aaa-override
Device(config-wlan)# nac
```

This example shows how to disable RADIUS NAC on the WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no nac
Device(config-wlan)# no aaa-override
```

nas-id option2

To configure option 2 parameters for a NAS-ID, use the **nas-id option2** command.

nas-id option2 {**sys-ip** | **sys-name** | **sys-mac** }

Syntax Description

sys-ip	System IP Address.
sys-name	System Name.
sys-mac	System MAC address.

Command Default

None

Command Modes

config-aaa-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the system IP address for the NAS-ID:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless aaa policy profile-name
Device(config-aaa-policy)# nas-id option2 sys-ip
```

network

To configure the network number in decimal notation, use the **network** command.

network *network-number* [{*network-mask* | **secondary** }]

Syntax Description

ipv4-address	Network number in dotted-decimal notation.
network-mask	Network mask or prefix length.
secondary	Configure as secondary subnet.

Command Default

None

Command Modes

dhcp-config

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure network number and the mask address:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip dhcp pool name
Device(dhcp-config)# network 209.165.200.224 255.255.255.0
```

nmsp cloud-services enable

To configure NMSP cloud services, use the **nmsp cloud-services enable** command.

nmsp cloud-services enable

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to enable NMSP cloud services:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# nmsp cloud-services enable
```

nmsp cloud-services http-proxy

To configure the proxy for NMSP cloud server, use the **nmsp cloud-services http-proxy** command.

nmsp cloud-services http-proxy *proxy-server port*

Syntax Description

proxy-server	Enter the hostname or the IP address of the proxy server for NMSP cloud services.
port	Enter the proxy server port number for NMSP cloud services.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the proxy for NMSP cloud server:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# nmsp cloud-services http-proxy host-name port-number
```

nmsp cloud-services server token

To configure the NMSP cloud services server parameters, use the **nmsp cloud-services server token** command.

nmsp cloud-services server token *token*

Syntax Description

token	Authentication token for the NMSP cloud services.

Command Default

None

Command Modes

config

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the for the NMSP cloud services server parameters:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# nmsp cloud-services server token authentication-token
```

nmsp cloud-services server url

To configure NMSP cloud services server URL, use the **nmsp cloud-services server url** command.

nmsp cloud-services server url *url*

Syntax Description

url	URL of the NMSP cloud services server.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure a URL for NMSP cloud services server:

```
Device(config)# nmps cloud-services server url http://www.example.com
```

nmsp notification interval

To modify the Network Mobility Services Protocol (NMSP) notification interval value on the controller to address latency in the network, use the **nmsp notification interval** command in global configuration mode.

nmsp notification interval { **attachment** | **location** | **rssi** {**clients** | **rfid** | **rogues** {**ap** | **client** } } }

Syntax Description

attachment	Specifies the time used to aggregate attachment information.
location	Specifies the time used to aggregate location information.
rssi	Specifies the time used to aggregate RSSI information.
clients	Specifies the time interval for clients.
rfid	Specifies the time interval for rfid tags.
rogues	Specifies the time interval for rogue APs and rogue clients .
ap	Specifies the time used to aggregate rogue APs .
client	Specifies the time used to aggregate rogue clients.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to set the NMSP notification interval for the active RFID tags to 25 seconds:

```
Device# configure terminal
Device(config)# nmsp notification-interval rfid 25
Device(config)# end
```

This example shows how to modify NMSP notification intervals for device attachment (connecting to the network or disconnecting from the network) every 10 seconds:

```
Device# configure terminal
Device(config)# nmsp notification-interval attachment 10
Device(config)# end
```

This example shows how to configure NMSP notification intervals for location parameters (location change) every 20 seconds:

```
Device# configure terminal
Device(config)# nmsp notification-interval location 20
Device(config)# end
```

nmsp strong-cipher

To enable the new ciphers, use the **nmsp strong-cipher** command in global configuration mode. To disable, use the **no** form of this command.

nmsp strong-cipher
no nmsp strong-cipher

Syntax Description

This command has no arguments or keywords.

Command Default

The new ciphers are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)E	This command was introduced.

Usage Guidelines

The **nmsp strong-cipher** command enables strong ciphers for new Network Mobility Service Protocol (NMSP) connections.

Note The existing NMSP connections will use the default cipher.

Examples

The following example shows how to enable a strong-cipher for NMSP:

```
Device> enable
Device> configure terminal
Device(config)# nmsp strong-cipher
```

Related Commands

Command	Description
show nmsp status	Displays the status of active NMSP connections.

option

To configure optional data parameters for a flow exporter for , use the **option** command in flow exporter configuration mode. To remove optional data parameters for a flow exporter, use the **no** form of this command.

option {**exporter-stats** | **interface-table** | **sampler-table**} [{**timeout** *seconds*}]
no option {**exporter-stats** | **interface-table** | **sampler-table**}

Syntax Description

exporter-stats	Configures the exporter statistics option for flow exporters.
interface-table	Configures the interface table option for flow exporters.
sampler-table	Configures the export sampler table option for flow exporters.
timeout *seconds*	(Optional) Configures the option resend time in seconds for flow exporters. The range is 1 to 86400. The default is 600.

Command Default

The timeout is 600 seconds. All other optional data parameters are not configured.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

The **option exporter-stats** command causes the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent. This command allows the collector to estimate packet loss for the export records it receives. The optional timeout alters the frequency at which the reports are sent.

The **option interface-table** command causes the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names. The optional timeout can alter the frequency at which the reports are sent.

The **option sampler-table** command causes the periodic sending of an options table, which details the configuration of each sampler and allows the collector to map the sampler ID provided in any flow record to a configuration that it can use to scale up the flow statistics. The optional timeout can alter the frequency at which the reports are sent.

To return this command to its default settings, use the **no option** or **default option** flow exporter configuration command.

The following example shows how to enable the periodic sending of the sampler option table, which allows the collector to map the sampler ID to the sampler type and rate:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option sampler-table
```

The following example shows how to enable the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option exporter-stats
```

The following example shows how to enable the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option interface-table
```

parameter-map type subscriber attribute-to-service

To configure parameter map type and name, use the **parameter-map type subscriber attribute-to-service** command.

parameter-map type subscriber attribute-to-service *parameter-map-name*

Syntax Description

attribute-to-service	Name the attribute to service.
parameter-map-name	Name of the parameter map. The map name is limited to 33 characters.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure parameter map type and name:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type subscriber attribute-to-service parameter-map-name
```

password encryption aes

To enable strong (AES) password encryption, use the **password encryption aes** command. To disable this feature, use the **no** form of this command.

password encryption aes
`no password encryption aes`

Syntax Description

password	Configures the encryption password (key).
encryption	Encrypts system passwords.
aes	Enables stronger (AES) password encryption.

Command Default

None

Command Modes

Global configuration mode.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

The following example shows how to enable AES password encryption :

```
Device(config)#password encryption aes
```

peer-blocking

To configure peer-to-peer blocking on a WLAN, use the **peer-blocking** command. To disable peer-to-peer blocking, use the **no** form of this command.

peer-blocking {**drop** | **forward-upstream**}
no peer-blocking

Syntax Description

drop	Specifies the switch to discard the packets.
forward-upstream	Specifies the packets to be forwarded on the upstream VLAN. The device next in the hierarchy to the switch decides what action to take regarding the packets.

Command Default

Peer blocking is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable the drop and forward-upstream options for peer-to-peer blocking:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1

Device(config-wlan)# peer-blocking  drop
Device(config-wlan)# peer-blocking forward-upstream
```

This example shows how to disable the drop and forward-upstream options for peer-to-peer blocking:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1

Device(config-wlan)# no peer-blocking  drop
Device(config-wlan)# no peer-blocking forward-upstream
```

policy

To configure media stream admission policy, use the **policy** command.

policy {**admit** | **deny**}

Syntax Description

admit	Allows traffic for a media stream group.
deny	Denies traffic for a media stream group.

Command Default

None

Command Modes

media-stream

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to allow traffic for a media stream group:

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group ms-group 224.0.0.0 224.0.0.223
Device(media-stream)# policy admit
```

police

To define a policer for classified traffic, use the **police** command in policy-map class configuration mode. Use the **no** form of this command to remove an existing policer.

police *rate-bps burst-byte* [**conform-action transmit**]
no police rate-bps *burst-byte* [**conform-action transmit**]

Syntax Description

rate-bps	Specify the average traffic rate in bits per second (b/s). The range is 1000000 to 1000000000.
burst-byte	Specify the normal burst size in bytes. The range is 8000 to 1000000.
conform-action transmit	(Optional) When less than the specified rate, specify that the switch transmits the packet.

Command Default

No policers are defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded.

When configuring hierarchical policy maps, you can only use the **police** policy-map command in a secondary interface-level policy map.

The port ASIC device, which controls more than one physical port, supports 256 policers on the switch (255 user-configurable policers plus 1 policer reserved for internal use). The maximum number of configurable policers supported per port is 63. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port. There is no guarantee that a port will be assigned to any policer.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Examples

This example shows how to configure a policer that transmits packets if traffic is less than 1 Mb/s average rate with a burst size of 20 KB. There is no packet modification.

```
Device(config)# class-map class1
Device(config-cmap)# exit
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example shows how to configure a policer that transmits packets if traffic is less than 1 Mb/s average rate with a burst size of 20 KB. There is no packet modification. This example uses an abbreviated syntax:

```
Device(config)# class-map class1
Device(config-cmap)# exit
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# police 1m 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example shows how to configure a policer, which marks down the DSCP values with the values defined in policed-DSCP map and sends the packet:

```
Device(config)# policy-map policy2
Device(config-pmap)# class class2
Device(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Device(config-pmap-c)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

police cir

To set the policing of committed information rate, use the **police cir** command.

police cir *<target bit rate>*

Syntax Description

police cir	Polices committed information rate.
8000-10000000000	Sets the target bit rate at bits per second. The range is between 8000 and 10000000000.

Command Default

None

Command Modes

Policy map class configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

Example

This example shows how to set the committed information rate:

```
Device(config-pmap-c)#police cir 8000
```

policy-map

To create or modify a policy map that can be attached to multiple physical ports or switch virtual interfaces (SVIs) and to enter policy-map configuration mode, use the **policy-map** command in global configuration mode. Use the **no** form of this command to delete an existing policy map and to return to global configuration mode.

policy-map *policy-map-name*
no policy-map *policy-map-name*

Syntax Description

policy-map-name	Name of the policy map.

Command Default

No policy maps are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class**—Defines the classification match criteria for the specified class map.
- **description**—Describes the policy map (up to 200 characters).
- **exit**—Exits policy-map configuration mode and returns you to global configuration mode.
- **no**—Removes a previously defined policy map.
- **sequence-interval**—Enables sequence number capability.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created, added to, or modified. Entering the **policy-map** command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands. You define packet classification on a physical-port basis.

Only one policy map per ingress port is supported. You can apply the same policy map to multiple physical ports.

You can apply a nonhierarchical policy maps to physical ports. A nonhierarchical policy map is the same as the port-based policy maps in the switch.

A hierarchical policy map has two levels in the format of a parent-child policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suit the QoS configuration.

In VLAN-based QoS, a service policy is applied to an SVI interface.

Note Not all MQC QoS combinations are supported for wired ports. For information about these restrictions, see chapters "Restrictions for QoS on Wired Targets" in the QoS configuration guide.

Examples

This example shows how to create a policy map called policy1. When attached to the ingress port, it matches all the incoming traffic defined in class1, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic less than the profile is sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example show you how to configure hierarchical polices:

```
Device# configure terminal
Device(config)# class-map c1
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class c2
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
Device(config-pmap-c)# service-policy child
Deviceconfig-pmap-c)# end
```

This example shows how to delete a policy map:

```
Device(config)# no policy-map policymap2
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

policy-map

To create or modify a policy map that can be attached to multiple physical ports or switch virtual interfaces (SVIs) and to enter policy-map configuration mode, use the **policy-map** command in global configuration mode. Use the **no** form of this command to delete an existing policy map and to return to global configuration mode.

policy-map *policy-map-name*
no policy-map *policy-map-name*

Syntax Description

policy-map-name	Name of the policy map.

Command Default

No policy maps are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class**—Defines the classification match criteria for the specified class map.
- **description**—Describes the policy map (up to 200 characters).
- **exit**—Exits policy-map configuration mode and returns you to global configuration mode.
- **no**—Removes a previously defined policy map.
- **sequence-interval**—Enables sequence number capability.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created, added to, or modified. Entering the **policy-map** command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands. You define packet classification on a physical-port basis.

Only one policy map per ingress port is supported. You can apply the same policy map to multiple physical ports.

You can apply a nonhierarchical policy maps to physical ports. A nonhierarchical policy map is the same as the port-based policy maps in the switch.

A hierarchical policy map has two levels in the format of a parent-child policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suit the QoS configuration.

In VLAN-based QoS, a service policy is applied to an SVI interface.

Note Not all MQC QoS combinations are supported for wired ports. For information about these restrictions, see chapters "Restrictions for QoS on Wired Targets" in the QoS configuration guide.

Examples

This example shows how to create a policy map called policy1. When attached to the ingress port, it matches all the incoming traffic defined in class1, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic less than the profile is sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example show you how to configure hierarchical polices:

```
Device# configure terminal
Device(config)# class-map c1
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class c2
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
Device(config-pmap-c)# service-policy child
Deviceconfig-pmap-c)# end
```

This example shows how to delete a policy map:

```
Device(config)# no policy-map policymap2
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

port

To configure the port number to use when configuring the custom application, use the **port** command.

port *port-no*

Syntax Description

port-no	Port number.

Command Default

None

Command Modes

config-custom

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the port number to use when configuring the custom application:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip nbar custom custom-protocol http host host-string
Device(config-custom)# http host hostname
Device(config-custom)# port port-no
```

priority priority-value

To configure media stream priority, use the **priority** *priority-value* command.

priority *priority-value*

Syntax Description

priority-value	Media stream priority value. Valid range is 1 to 8, with 1 being lowest priority and 8 being highest priority.

Command Default

None

Command Modes

config-media-stream

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to set the media stream priority value to the highest, that is 8:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# priority 8
```

public-ip

To configure the NAT public IP address of the controller, use the **public-ip** command.

public-ip { *ipv4-address* | *ipv6-address* }

Syntax Description

ipv4-address	Sets IPv4 address.
ipv6-address	Sets IPv6 address.

Command Default

None

Command Modes

Management Interface Configuration(config-mgmt-interface)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

Example

The following example shows how to configure the NAT public IP address of the controller:

```
Device# configure terminal
Device(config)# wireless management interface Vlan1
Device(config-mgmt-interface)# public-ip 192.168.172.100
```

qos video

To configure over-the-air QoS class to video only, use the **qos video** command.

qos video

Command Default None

Command Modes config-media-stream

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure over-the-air QoS class to video only:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# qos video
```

radius server

To configure the RADIUS server, use the **radius server** command in global configuration mode.

radius server *server-name*

Syntax Description

server-name	RADIUS server name.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None

The following example shows how to configure a radius server:

```
Device(config)# radius server ISE
```

radius-server attribute wireless accounting call-station-id

To configure call station identifier sent in the RADIUS accounting messages, use the **radius-server attribute wireless accounting call-station-id** command. To remove the call station identifier from the radius accounting messages, use the **no** form of the command.

radius-server attribute wireless authentication call-station-id { **ap-ethmac-only** | **ap-ethmac-ssid** | **ap-ethmac-ssid-flexprofilename** | **ap-ethmac-ssid-policytagname** | **ap-ethmac-ssid-sitetagname** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-macaddress** | **ap-macaddress-ssid** | **ap-macaddress-ssid-flexprofilename** | **ap-macaddress-ssid-policytagname** | **ap-macaddress-ssid-sitetagname** | **ap-name** | **ap-name-ssid** | **flex-profile-name** | **ipaddress** | **macaddress** | **policy-tag-name** | **site-tag-name** | **vlan-id** }

Syntax Description

ap-ethmac-only	Sets the call station identifier type to be AP's radio MAC address.
ap-ethmac-ssid	Sets the call station identifier type AP's radio MAC address with SSID.
ap-ethmac-ssid-flexprofilename	Sets the call station identifier type AP's radio MAC address with SSID and flex profile name.
ap-ethmac-ssid-policytagname	Sets the call station identifier type AP's radio MAC address with SSID and policy tag name.
ap-ethmac-ssid-sitetagname	Sets the call station identifier type AP's radio MAC address with SSID and site tag name.
ap-group-name	Sets the call station identifier type to use the AP group name.
ap-label-address	Sets the call station identifier type to the AP's radio MAC address that is printed on the AP label.
ap-label-address-ssid	Sets the call station identifier type to the AP's radio MAC address and SSID that is printed on the AP label.
ap-location	Sets the call station identifier type to the AP location.
ap-macaddress	Sets the call station identifier type to the AP's radio MAC address.
ap-macaddress-ssid	Sets the call station identifier type to the AP's radio MAC address with SSID.
ap-macaddress-ssid-flexprofilename	Sets the call station identifier type to the AP's radio MAC address with SSID and flex profile name.
ap-macaddress-ssid-policytagname	Sets the call station identifier type to the AP's radio MAC address with SSID and policy tag name.
ap-macaddress-ssid-sitetagname	Sets the call station identifier type to the AP's radio MAC address with SSID and site tag name.
ap-name	Sets the call station identifier type to the AP name.

ap-name-ssid	Sets the call station identifier type to the AP name with SSID.
flex-profile-name	Sets the call station identifier type to the flex profile name.
ipaddress	Sets the call station identifier type to the IP address of the system.
macaddress	Sets the call station identifier type to the MAC address of the system.
policy-tag-name	Sets the call station identifier type to the policy tag name.
site-tag-name	Sets the call station identifier type to the site tag name.
vlan-id	Sets the call station identifier type to the system's VLAN ID.

Command Default

Call station identifier is not configured.

Command Modes

Global Configuration(config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Cisco IOS XE Bengaluru 17.4.1	This command was modified. The **policy-tag-name**, **flex-profile-name**, **ap-macaddress-ssid-flexprofilename**, **ap-macaddress-ssid-policytagname**, **ap-macaddress-ssid-sitetagname**, **ap-ethmac-ssid-flexprofilename**, **ap-ethmac-ssid-policytagname**, and **ap-ethmac-ssid-sitetagname** keywords were introduced.

Usage Guidelines

Example

The following example shows how to configure a call station identifier sent in the RADIUS accounting messages:

```
Device(config)# radius-server attribute wireless accounting call-station-id site-tag-name
```

radius-server attribute wireless authentication call-station-id

To configure call station identifier sent in the RADIUS authentication messages, use the **radius-server attribute wireless authentication call-station-id** command. To remove the call station identifier from the radius accounting messages, use the **no** form of the command.

radius-server attribute wireless authentication call-station-id { **ap-ethmac-only** | **ap-ethmac-ssid** | **ap-ethmac-ssid-flexprofilename** | **ap-ethmac-ssid-policytagname** | **ap-ethmac-ssid-sitetagname** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-macaddress** | **ap-macaddress-ssid** | **ap-macaddress-ssid-flexprofilename** | **ap-macaddress-ssid-policytagname** | **ap-macaddress-ssid-sitetagname** | **ap-name** | **ap-name-ssid** | **flex-profile-name** | **ipaddress** | **macaddress** | **policy-tag-name** | **site-tag-name** | **vlan-id** }

Syntax Description

ap-ethmac-only	Sets the call station identifier type to be AP's radio MAC address.
ap-ethmac-ssid	Sets the call station identifier type AP's radio MAC address with SSID.
ap-ethmac-ssid-flexprofilename	Sets the call station identifier type AP's radio MAC address with SSID and flex profile name.
ap-ethmac-ssid-policytagname	Sets the call station identifier type AP's radio MAC address with SSID and policy tag name.
ap-ethmac-ssid-sitetagname	Sets the call station identifier type AP's radio MAC address with SSID and site tag name.
ap-group-name	Sets the call station identifier type to use the AP group name.
ap-label-address	Sets the call station identifier type to the AP's radio MAC address that is printed on the AP label.
ap-label-address-ssid	Sets the call station identifier type to the AP's radio MAC address and SSID that is printed on the AP label.
ap-location	Sets the call station identifier type to the AP location.
ap-macaddress	Sets the call station identifier type to the AP's radio MAC address.
ap-macaddress-ssid	Sets the call station identifier type to the AP's radio MAC address with SSID.
ap-macaddress-ssid-flexprofilename	Sets the call station identifier type to the AP's radio MAC address with SSID and flex profile name.
ap-macaddress-ssid-policytagname	Sets the call station identifier type to the AP's radio MAC address with SSID and policy tag name.
ap-macaddress-ssid-sitetagname	Sets the call station identifier type to the AP's radio MAC address with SSID and site tag name.
ap-name	Sets the call station identifier type to the AP name.

ap-name-ssid	Sets the call station identifier type to the AP name with SSID.
flex-profile-name	Sets the call station identifier type to the flex profile name.
ipaddress	Sets the call station identifier type to the IP address of the system.
macaddress	Sets the call station identifier type to the MAC address of the system.
policy-tag-name	Sets the call station identifier type to the policy tag name.
site-tag-name	Sets the call station identifier type to the site tag name.
vlan-id	Sets the call station identifier type to the system's VLAN ID.

Command Default

Call station identifier is not configured.

Command Modes

Global Configuration(config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Cisco IOS XE Bengaluru 17.4.1	This command was modified. The **policy-tag-name**, **flex-profile-name**, **ap-macaddress-ssid-flexprofilename**, **ap-macaddress-ssid-policytagname**, **ap-macaddress-ssid-sitetagname**, **ap-ethmac-ssid-flexprofilename**, **ap-ethmac-ssid-policytagname**, and **ap-ethmac-ssid-sitetagname** keywords were introduced.

Usage Guidelines

Example

The following example shows how to configure a call station identifier sent in the RADIUS authentication messages:

```
Device(config)# radius-server attribute wireless authentication call-station-id site-tag-name
```

range

To configure range from MAP to RAP bridge, use the **range** command.

range *range-in-feet*

Syntax Description

range-in-feet	Configure the range value in terms of feet. Valid range is from 150 feet to 132000 feet.

Command Default

1200

Command Modes

config-wireless-mesh-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure range from MAP to RAP bridge for a mesh AP profile:

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# range 300
```

record wireless avc basic

To apply the *wireless avc basic* AVC flow record to a flow monitor, use the **record wireless avc basic** command.

record wireless avc basic

Command Default None

Command Modes config-flow-monitor

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines This command specifies the basic wireless AVC template. When you are configuring AVC, you will need to create a flow monitor using the **record wireless avc basic** command.

Examples

The following example shows how to apply the *wireless avc basic* AVC flow record to a flow monitor named *test-flow*:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# flow monitor test-flow
Device(config-flow-monitor)# record wireless avc basic
```

redirect

To configure a redirect to an external portal, use the **redirect** command.

redirect {**for-login** | **on-failure** | **on-success** }*redirect-url-name*

Syntax Description

for-login	To login, redirect to this URL.
on-failure	If login fails, redirect to this URL.
on-success	If login is sucessful, redirect to this URL.
redirect-url-name	Redirect URL name.

Command Default

None

Command Modes

config-params-parameter-map

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure an redirect to an external IPv4 URL to login:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-name
Device(config-params-parameter-map)# redirect for-login cisco.com
```

redirect portal

To configure external IPv4 or IPv6 portal, use the **redirect portal** command.

redirect portal {**ipv4** | **ipv6** }*ip-addr*

Syntax Description

ipv4	IPv4 portal address
ipv6	IPv6 portal address

Command Default

None

Command Modes

config-params-parameter-map

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure an external IPv4 portal address:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-name
Device(config-params-parameter-map)# redirect portal ipv4 192.168.1.100
```

remote-lan

To map an RLAN policy profile to an RLAN profile, use the **remote-lan** command.

remote-lan *remote-lan-profile-name* **policy** *rlan-policy-profile-name* **port-id** *port-id*

Syntax Description

remote-lan-profile-name	Remote LAN profile name.
rlan-policy-profile-name	Remote LAN policy profile name.
port-id	Port ID.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to map an RLAN policy profile to an RLAN profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless tag policy remote-lan-policy-tag
Device(config-policy-tag)# remote-lan rlan_profile_name policy rlan_policy_profile port-id
 2
Device(config-policy-tag)# end
```

request platform software trace archive

To archive all the trace logs relevant to all the processes running on a system since the last reload on the and to save this in the specified location, use the **request platform software trace archive** command in privileged EXEC or user EXEC mode.

request platform software trace archive [**last** *number-of-days* [**days** [**target** *location*]] | **target** *location*]

Syntax Description

last *number-of-days*	Specifies the number of days for which the trace files have to be archived.
target *location*	Specifies the location and name of the archive file.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

This archive file can be copied from the system, using the tftp or scp commands.

Examples

This example shows how to archive all the trace logs of the processes running on the since the last 5 days:

```
Device# request platform software trace archive last 5 days target flash:test_archive
```

rf tag

To configure an RF tag to the AP, use the **rf tag**command.

rf tag *rf-tag-name*

Syntax Description

rf-tag-name	RF tag name.

Command Default

None

Command Modes

config-ap-tag

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The AP will disconnect and rejoin after running this command.

Example

The following example shows how to configure an RF tag:

```
Device(config-ap-tag)# rf-tag rftag1
```

rrc-evaluation

To configure Resource Reservation Control (RRC) reevaluation admission, use the **rrc-evaluation** command.

rrc-evaluation {**initial** | **periodic**}

Syntax Description

initial	Configures initial admission evaluation.
periodic	Configures periodic admission evaluation.

Command Default

None

Command Modes

config-media-stream

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the RRC reevaluation admission to initial admission evaluation.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# rrc-evaluation initial
```

security

To configure mesh security, use the **security** command.

security { **eap** | **psk** }

Syntax Description

eap	Configure mesh security EAP for Mesh AP.
psk	Configure mesh security PSK for Mesh AP

Command Default

EAP

Command Modes

config-wireless-mesh-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure mesh security with EAP protcol on an Mesh AP:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile mesh profile-name
Device(config-wireless-mesh-profile)# security eap
```

security dot1x authentication-list

To configure security authentication list for IEEE 802.1x, use the **security dot1x authentication-list** *auth-list-name* command.

security dot1x authentication-list *auth-list-name*

Syntax Description

Parameter	Description
auth-list-name	Authentication list name.

Command Default

None

Command Modes

config-wlan

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure security authentication list for IEEE 802.1x:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan-name
Device(config-wlan)# security dot1x authentication-list auth-list-realm
```

security ft

To configure 802.11r fast transition parameters, use the **security ft** command. To configure fast transition **over the air**, use the **no security ft over-the-ds** command.

security ft [{**over-the-ds** | **reassociation-timeout** *timeout-jn-seconds*}]
no security ft [{**over-the-ds** | **reassociation-timeout**}]

Syntax Description

over-the-ds	(Optional) Specifies that the 802.11r fast transition occurs over a distributed system. The no form of the command with this parameter configures security ft over the air.
reassociation-timeout	(Optional) Configures the reassociation timeout interval.
timeout-in-seconds	(Optional) Specifies the reassociation timeout interval in seconds. The valid range is between 1 to 100. The default value is 20.

Command Default

The feature is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None

WLAN Security must be enabled.

Example

The following example configures security FT configuration for an open WLAN:

```
Device#wlan test
Device(config-wlan)# client vlan 0140
Device(config-wlan)# no mobility anchor sticky
Device(config-wlan)# no security wpa
Device(config-wlan)# no security wpa akm dot1x
Device(config-wlan)# no security wpa wpa2
Device(config-wlan)# no security wpa wpa2 ciphers aes
Device(config-wlan)# security ft
Device(config-wlan)# shutdown
```

The following example shows a sample security FT on a WPA-enabled WLAN:

```
Device# wlan test
Device(config-wlan)# client vlan 0140
Device(config-wlan)# no security wpa akm dot1x
Device(config-wlan)# security wpa akm ft psk
Device(config-wlan)# security wpa akm psk set-key ascii 0 test-test
```

```
Device(config-wlan)# security ft
Device(config-wlan)# no shutdown
```

security pmf

To configure 802.11w Management Frame Protection (PMF) on a WLAN, use the **security pmf** command. To disable management frame protection, use the **no** form of the command.

security pmf {**association-comeback** *association-comeback-time-seconds* | **mandatory** | **optional** | **saquery-retry-time** *saquery-retry-time-milliseconds*}
no security pmf [{**association-comeback** *association-comeback-time-seconds* | **mandatory** | **optional** | **saquery-retry-time** *saquery-retry-time-milliseconds*}]

Syntax Description

association-comeback	Configures the 802.11w association comeback time.
association-comeback-time-seconds	Association comeback interval in seconds. Time interval that an associated client must wait before the association is tried again after it is denied with a status code 30. The status code 30 message is "Association request rejected temporarily; Try again later." The range is from 1 through 20 seconds.
mandatory	Specifies that clients are required to negotiate 802.1w PMF protection on the WLAN.
optional	Specifies that the WLAN does not mandate 802.11w support on clients. Clients with no 802.11w capability can also join.
saquery-retry-time	Time interval identified before which the SA query response is expected. If the switch does not get a response, another SA query is tried.
saquery-retry-time-milliseconds	The saquery retry time in milliseconds. The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds.

Command Default

PMF is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

You must have WPA (Wi-Fi Protected Access) and AKM (Authentication Key Management) configured to use this feature. See Related Command section for more information on configuring the security parameters.

802.11w introduces an Integrity Group Temporal Key (IGTK) that is used to protect broadcast or multicast robust management frames. IGTK is a random value, assigned by the authenticator station (switch) used to protect MAC management protocol data units (MMPDUs) from the source STA. The 802.11w IGTK key is

derived using the four-way handshake and is used only on WLANs that are configured with WPA2 security at Layer 2.

This example shows how to enable the association comeback value at 15 seconds.

```
Device(config-wlan)# security pmf association-comeback 15
```

This example shows how to configure mandatory 802.11w MPF protection for clients on a WLAN:

```
Device(config-wlan)# security pmf mandatory
```

This example shows how to configure optional 802.11w MPF protection for clients on a WLAN:

```
Device(config-wlan)# security pmf optional
```

This example shows how to configure the saquery parameter:

```
Device(config-wlan)# security pmf saquery-retry-time 100
```

This example shows how to disable the PMF feature:

```
Device(config-wlan)# no security pmf
```

security static-wep-key

To configure static WEP keys on a WLAN, use the **security static-wep-key** command.

security static-wep-key {**authentication** {**open** | **sharedkey** } | **encryption** {**104** | **40** }{**ascii** | **hex** | {**0** | **8** }*wep-key* | **wep-index** }}

Syntax Description

open	Open system authentication.
sharedkey	Shared key authentication.
0	Specifies an UNENCRYPTED password is used.
8	Specifies an AES encrypted password is used.
wep-key	Enter the name of the WEP key.

Command Default

None

Command Modes

config-wlan

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to authenticate 802.11 using shared key:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan profile-name wlan-id
Device(config-wlan)# security static-wep-key authentication sharedkey
```

security web-auth

To change the status of web authentication used on a WLAN, use the **security web-auth** command. To disable web authentication on a WLAN, use the **no** form of the command.

security web-auth [{**authentication-list** *authentication-list-name* | **on-macfilter-failure** | **parameter-map** *parameter-map-name*}]
no security web-auth [{**authentication-list** [**authentication-list-name**] | **on-macfilter-failure** | **parameter-map** [**parameter-name**]}]

Syntax Description

authentication-list *authentication-list-name*	Sets the authentication list for IEEE 802.1x.
on-macfilter-failure	Enables web authentication on MAC failure.
parameter-map *parameter-map-name*	Configures the parameter map.

Command Default

Web authentication is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Examples

The following example shows how to configure the authentication-list web authentication on a WLAN:

```
Device(config-wlan)# security web-auth authentication-list test
```

security wpa akm

To configure authentication key management using Cisco Centralized Key Management (CCKM), use the **security wpa akm** command. To disable the authentication key management for Cisco Centralized Key Management, use the **no** form of the command.

security wpa [{**akm** {**cckm** | **dot1x** | **ft** | **pmf** | **psk**} | **wpa1** [**ciphers** {**aes** | **tkip**}] | **wpa2** [**ciphers** {**aes** | **tikp**}]}]
no security wpa [{**akm** {**cckm** | **dot1x** | **ft** | **pmf** | **psk**} | **wpa1** [**ciphers** {**aes** | **tkip**}] | **wpa2** [**ciphers** {**aes** | **tikp**}]}]

Syntax Description

akm	Configures the Authentication Key Management (AKM) parameters.
aes	Configures AES (Advanced Encryption Standard) encryption support.
cckm	Configures Cisco Centralized Key Management support.
ciphers	Configures WPA ciphers.
dot1x	Configures 802.1x support.
ft	Configures fast transition using 802.11r.
pmf	Configures 802.11w management frame protection.
psk	Configures 802.11r fast transition pre-shared key (PSK) support.
tkip	Configures Temporal Key Integrity Protocol (TKIP) encryption support.
wpa2	Configures Wi-Fi Protected Access 2 (WPA2) support.

Command Default

By default Wi-Fi Protected Access2, 802.1x are enabled. WPA2, PSK, CCKM, FT dot1x, FT PSK, PMF dot1x, PMF PSK, FT Support are disabled. The FT Reassociation timeout is set to 20 seconds, PMF SA Query time is set to 200.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Example

The following example shows how to configure CCKM on the WLAN.

```
Device(config-wlan)#security wpa akm cckm
```

service-policy (WLAN)

To configure the WLAN quality of service (QoS) service policy, use the **service-policy** command. To disable a QoS policy on a WLAN, use the **no** form of this command.

service-policy [**client**] {**input** | **output**} *policy-name*
no service-policy [**client**] {**input** | **output**} *policy-name*

Syntax Description

client	(Optional) Assigns a policy map to all clients in the WLAN.
input	Assigns an input policy map.
output	Assigns an output policy map.
policy-name	The policy name.

Command Default

No policies are assigned and the state assigned to the policy is None.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Examples

This example shows how to configure the input QoS service policy on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# service-policy input policy-test
```

This example shows how to disable the input QoS service policy on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no service-policy input policy-test
```

This example shows how to configure the output QoS service policy on a WLAN to platinum (precious metal policy):

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# service-policy output platinum
```

service-policy qos

To configure a QoS service policy, use the **service-policy qos** command.

service-policy qos {**input** | **output**}*policy-name*

Syntax Description

input	Input QoS policy.
output	Output QoS policy.
policy-name	Policy name.

Command Default

None

Command Modes

config-service-template

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure an output QoS policy:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# service-template fabric-profile-name
Device(config-service-template)# service-policy qos output policy-name
```

service-template

To configure service template, use the **service-template** command.

service-template *service-template-name* {**access-group** *acl_list* | **vlan** *vlan_id* | **absolute-timer** *seconds* | **service-policy qos** {**input** | **output**}}

Syntax Description

service-template-name	Name of the service template.
acl_list	Access list name to be applied.
vlan_id	VLAN ID. The VLAN ID value ranges from 1 to 4094.
seconds	Session timeout value for service template. The session timeout value ranges from 1 to 65535 seconds.
service-policy qos {**input** | **output**	QoS policies for client.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None

The following example shows how to configure service template:

```
Device#configure terminal
Device(config)#service-template cisco-phone-template
Device(config-service-template)#access-group foo-acl
Device(config-service-template)#vlan 100
Device(config-service-template)#service-policy qos input foo-qos
Device(config-service-template)#end
```

service timestamps

To configure the system to time-stamp debugging or logging messages, use the**service timestamps** command in global configuration commands. Use the **no** form of this command to disable this service.

service timestamps debug log{**datetime** | **uptime***localtimemsecshow-timezoneyear*}
no service timestamps debuglog

Syntax Description

debug	Debug as the timestamp message type.
log	Log as the timestamp message type.
datetime	**datetime**
uptime	(Optional) Time stamp with time since the system was rebooted.
localtime	(Optional) Time stamp relative to the local time zone.
msec	(Optional) Include milliseconds in the date and time stamp.
show-timezone	(Optional) Include the time zone name in the time stamp.
year	(Optional) Include year in timestamp.

Command Default

No time-stamping.

If **service timestamps** is specified with no arguments or keywords, default is **service timestamps debug uptime**.

The default for **service timestamps debugdatetime** is to format the time in UTC, with no milliseconds and no time zone name.

The command **no service timestamps** by itself disables time stamps for both debug and log messages.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.1.1s.

Usage Guidelines

Time stamps can be added to either debugging or logging messages independently. The uptime form of the command adds time stamps in the format HHHH:MM:SS, indicating the time since the system was rebooted. The datetime form of the command adds time stamps in the format MMM DD HH:MM:SS, indicating the date and time according to the system clock. If the system clock has not been set, the date and time are preceded by an asterisk (*) to indicate that the date and time are probably not correct.

Example

The following example enables time stamps on debugging messages, showing the time since reboot:

```
Device(config)# service timestamps debug uptime
```

The following example enables time stamps on logging messages, showing the current time and date relative to the local time zone, with the time zone name included:

```
Device(config)# service timestamps log datetime localtime show-timezone
```

session-timeout

To configure session timeout for clients associated to a WLAN, use the **session-timeout** command. To disable a session timeout for clients that are associated to a WLAN, use the **no** form of this command.

session-timeout seconds
no session-timeout

Syntax Description

seconds	Timeout or session duration in seconds. The range is from 300 to 86400. Configuring 86400 is equivalent to max timeout. And value 0 is not recommended.

Command Default

The client timeout is set to 1800 seconds for WLANs that are configured with dot1x security. The client timeout is set to 0 for open WLANs.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure a session timeout to 300 seconds:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# session-timeout 300
```

This example shows how to disable a session timeout:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no session-timeout
```

set

To classify IP traffic by setting a Differentiated Services Code Point (DSCP) or an IP-precedence value in the packet, use the **set** command in policy-map class configuration mode. Use the **no** form of this command to remove traffic classification.

set
cos | **dscp** | **precedence** | **ip** | **qos-group** | **wlan**
set cos
{*cos-value* } | {**cos** | **dscp** | **precedence** | **qos-group** | **wlan**} [{**table** *table-map-name*}]
set dscp
{*dscp-value* } | {**cos** | **dscp** | **precedence** | **qos-group** | **wlan**} [{**table** *table-map-name*}]
set ip {**dscp** | **precedence**}
set precedence {*precedence-value* } | {**cos** | **dscp** | **precedence** | **qos-group**} [{**table** *table-map-name*}]
set qos-group
{*qos-group-value* | **dscp** [{**table** *table-map-name*}] | **precedence** [{**table** *table-map-name*}]}
set wlan user-priority
user-priority-value | **costable** *table-map-name* | **dscptable** *table-map-name* | **qos-grouptable** *table-map-name* | **wlantable** *table-map-name*

Syntax Description

cos	Sets the Layer 2 class of service (CoS) value or user priority of an outgoing packet. You can specify these values:
	• *cos-value*—CoS value from 0 to 7. You also can enter a mnemonic name for a commonly used value.
	• Specify a packet-marking category to set the CoS value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords:
	  • **cos**—Sets a value from the CoS value or user priority.
	  • **dscp**—Sets a value from packet differentiated services code point (DSCP).
	  • **precedence**—Sets a value from packet precedence.
	  • **qos-group**—Sets a value from the QoS group.
	  • **wlan**—Sets the WLAN user priority values.
	• (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map are used to set the CoS value. Enter the name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters.
	If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the CoS value. For example, if you enter the **set cos precedence** command, the precedence (packet-marking category) value is copied and used as the CoS value.

dscp	Sets the differentiated services code point (DSCP) value to mark IP(v4) and IPv6 packets. You can specify these values:
	• *cos-value*—Number that sets the DSCP value. The range is from 0 to 63. You also can enter a mnemonic name for a commonly used value.
	• Specify a packet-marking category to set the DSCP value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords:
	  • **cos**—Sets a value from the CoS value or user priority.
	  • **dscp**—Sets a value from packet differentiated services code point (DSCP).
	  • **precedence**—Sets a value from packet precedence.
	  • **qos-group**—Sets a value from the QoS group.
	  • **wlan**—Sets a value from WLAN.
	• (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP value. Enter the name of the table map used to specify the DSCP value. The table map name can be a maximum of 64 alphanumeric characters.
	If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the DSCP value. For example, if you enter the **set dscp cos** command, the CoS value (packet-marking category) is copied and used as the DSCP value.

ip	Sets IP values to the classified traffic. You can specify these values: • **dscp**—Specify an IP DSCP value from 0 to 63 or a packet marking category. • **precedence**—Specify a precedence-bit value in the IP header; valid values are from 0 to 7 or specify a packet marking category.

precedence	Sets the precedence value in the packet header. You can specify these values:
	• *precedence-value*— Sets the precedence bit in the packet header; valid values are from 0 to 7. You also can enter a mnemonic name for a commonly used value.
	• Specify a packet marking category to set the precedence value of the packet.
	  • **cos**—Sets a value from the CoS or user priority.
	  • **dscp**—Sets a value from packet differentiated services code point (DSCP).
	  • **precedence**—Sets a value from packet precedence.
	  • **qos-group**—Sets a value from the QoS group.
	• (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the precedence value. Enter the name of the table map used to specify the precedence value. The table map name can be a maximum of 64 alphanumeric characters.
	If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the precedence value. For example, if you enter the **set precedence cos** command, the CoS value (packet-marking category) is copied and used as the precedence value.

qos-group	Assigns a QoS group identifier that can be used later to classify packets. • *qos-group-value*—Sets a QoS value to the classified traffic. The range is 0 to 31. You also can enter a mnemonic name for a commonly used value. • **dscp**—Sets the original DSCP field value of the packet as the QoS group value. • **precedence**—Sets the original precedence field value of the packet as the QoS group value. • (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP or precedence value. Enter the name of the table map used to specify the value. The table map name can be a maximum of 64 alphanumeric characters. If you specify a packet-marking category (**dscp** or **precedence**) but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the QoS group value. For example, if you enter the **set qos-group precedence** command, the precedence value (packet-marking category) is copied and used as the QoS group value.

wlan user-priority *wlan-user-priority*	Assigns a WLAN user-priority to the classified traffic. You can specify these values: • *wlan-user-priority*—Sets a WLAN user priority to the classified traffic. The range is 0 to 7. • **cos**—Sets the Layer 2 CoS field value as the WLAN user priority. • **dscp**—Sets the DSCP field value as the WLAN user priority. • **precedence**—Sets the precedence field value as the WLAN user priority. • **wlan**—Sets the WLAN user priority field value as the WLAN user priority. • (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the WLAN user priority value. Enter the name of the table map used to specify the value. The table map name can be a maximum of 64 alphanumeric characters. If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the WLAN user priority. For example, if you enter the **set wlan user-priority cos** command, the cos value (packet-marking category) is copied and used as the WLAN user priority.

Command Default

No traffic classification is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

For the **set dscp** *dscp-value* command, the **set cos** *cos-value* command, and the **set ip precedence** *precedence-value* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **set dscp af11** command, which is the same as entering the **set dscp 10** command. You can enter the **set ip precedence critical** command, which is the same as entering the **set ip precedence 5** command. For a list of supported mnemonics, enter the **set dscp ?** or the **set ip precedence ?** command to see the command-line help strings.

When you configure the **set dscp cos**command, note the following: The CoS value is a 3-bit field, and the DSCP value is a 6-bit field. Only the three bits of the CoS field are used.

When you configure the **set dscp qos-group** command, note the following:

- The valid range for the DSCP value is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 99.
- If a QoS group value falls within both value ranges (for example, 44), the packet-marking value is copied and the packets is marked.
- If QoS group value exceeds the DSCP range (for example, 77), the packet-marking value is not be copied and the packet is not marked. No action is taken.

The **set qos-group** command cannot be applied until you create a service policy in policy-map configuration mode and then attach the service policy to an interface or ATM virtual circuit (VC).

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Examples

This example shows how to assign DSCP 10 to all FTP traffic without any policers:

```
Device(config)# policy-map policy_ftp
Device(config-pmap)# class-map ftp_class
Device(config-cmap)# exit
Device(config)# policy policy_ftp
Device(config-pmap)# class ftp_class
Device(config-pmap-c)# set dscp 10
Device(config-pmap)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

sftp-image-path (image-download-mode sftp)

To configure the image path of the SFTP server for image download, use the **sftp-image-path** command. Use the **no** form of the command to negate the command or to set the command to its default.

`sftp-image-path`*sftp-image-path*

`no sftp-image-path`*sftp-image-path*

Syntax Description

sftp-image-path	Specifies the image path of the SFTP server.

Command Default

None

Command Modes

Wireless image download profile SFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode sftp
Device(config-wireless-image-download-profile-sftp)# sftp-image-path
/download/object/stream/images/ap-images
```

sftp-image-server (image-download-mode sftp)

To configure the SFTP server address for image download, use the **sftp-image-server** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
sftp-image-server {A.B.C.D | X:X:X:X::X}

no sftp-image-server {A.B.C.D | X:X:X:X::X}
```

Syntax Description

A.B.C.D	Specifies the SFTP IPv4 server address.
X:X:X:X::X	Specifies the SFTP IPv6 server address.

Command Default

None

Command Modes

Wireless image download profile SFTP configuration mode.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode sftp
Device(config-wireless-image-download-profile-sftp)# sftp-image-server 10.1.1.1
```

sftp-password (image-download-mode sftp)

To configure the SFTP server password for image dowload, use the **sftp-password** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
sftp-password {0| 8}<Enter password> <Re-enter password>

no sftp-password {0 | 8}<Enter password> <Re-enter password>
```

Syntax Description

0	Specifies that an unencrypted password will follow.
8	Specifies that an AES encrypted password will follow.
password	Specifies the SFTP server password.
re-enter password	Indicates that the user must re-enter the SFTP server password.

Command Default

None

Command Modes

Wireless image download profile SFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode sftp
Device(config-wireless-image-download-profile-sftp)# sftp-password 0 xxxxxxxx
```

sftp-password (trace-export)

To configure the SFTP server password for trace export, use the **sftp-password** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

`sftp-password<`*Enter password*`> <`*Re-enter password*`>`

`no sftp-password<`*Enter password*`> <`*Re-enter password*`>`

Syntax Description

password	Specifies the SFTP server password.
re-enter password	Indicates that the user must re-enter the SFTP server password.

Command Default

None

Command Modes

Wireless trace export profile SFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode sftp
Device(config-wireless-trace-export-profile-sftp)# sftp-password xxxxxxxx xxxxxxxx
```

sftp-path

To configure the path at the SFTP server for trace log export, use the **sftp-path** command. Use the **no** form of the command to negate the command or to set the command to its default.

`sftp-path`*sftp-path*

`no sftp-path`*sftp-path*

Syntax Description

sftp-path	Specifies the path at the SFTP server.

Command Default

None

Command Modes

Wireless trace export profile SFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode sftp
Device(config-wireless-trace-export-profile-sftp)# sftp-path
/download/object/stream/images/ap-images
```

sftp-server

To configure the SFTP server address for trace export, use the **sftp-server** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

`sftp-server{`*A.B.C.D* `|` *X:X:X:X::X*`}`

`no sftp-server {`*A.B.C.D* `|` *X:X:X:X::X*`}`

Syntax Description

A.B.C.D	Specifies the SFTP IPv4 server address.
X:X:X:X::X	Specifies the SFTP IPv6 server address.

Command Default

None

Command Modes

Wireless trace export profile SFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode sftp
Device(config-wireless-trace-export-profile-sftp)# sftp-server 10.1.1.1
```

sftp-username (image-download-mode sftp)

To configure the SFTP server username for image download, use the **sftp-username**command. Use the **no** form of this command to negate the configuration or to set the command to its default.

`sftp-username` *Username*

`no sftp-username` *Username*

Syntax Description

username	Specifies the SFTP server username.

Command Default

None

Command Modes

Wireless image download profile SFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode sftp
Device(config-wireless-image-download-profile-sftp)# sftp-username sftp-server-username
```

sftp-username (trace-export)

To configure the SFTP server username for trace export, use the **sftp-username**command. Use the **no** form of this command to negate the configuration or to set the command to its default.

`sftp-username` *Username*

`no sftp-username` *Username*

Syntax Description

username	Specifies the SFTP server username.

Command Default

None

Command Modes

Wireless trace export profile SFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode sftp
Device(config-wireless-trace-export-profile-sftp)# sftp-username sftp-server-username
```

tag rf

To configure a policy tag for an AP filter, use the **tag rf** command.

tag rf *rf-tag*

Syntax Description

rf-tag	RF tag name.

Command Default

None

Command Modes

config-ap-filter

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure a policy tag for an AP filter:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap filter name ap-filter-name
Device(config-ap-filter)# rf tag rf-tag-name
```

tag site

To configure a site tag for an AP filter, use the **tag site** *site-tag* command.

tag site *site-tag*

Syntax Description		
	site-tag	Name of the site tag.

Command Default None

Command Modes config-ap-filter

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure a site tag for an AP filter:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap filter name ap-filter-name
Device(config-ap-filter)# site tag site-tag-name
```

tftp-image-path (image-download-mode tftp)

To configure the image path at the TFTP server for image download, use the **tftp-image-path** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

`tftp-image-path` *tftp-image-path*

`no tftp-image-path` *tftp-image-path*

Syntax Description

tftp-image-path	Specifies the image path of the TFTP server.

Command Default

None

Command Modes

Wireless image dowload profile TFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode tftp
Device(config-wireless-image-download-profile-tftp)# tftp-image-path
/download/object/stream/images/ap-images
```

tftp-image-server (image-download-mode tftp)

To configure the TFTP server address for image download, use the **tftp-image-server** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
image-download-mode tftp

tftp-image-server {A.B.C.D | X:X:X:X::X}

no tftp-image-server {A.B.C.D | X:X:X:X::X}
```

Syntax Description

A.B.C.D	Specifies the TFTP IPv4 server address.
X:X:X:X::X	Specifies the TFTP IPv6 server address.

Command Default

None

Command Modes

Wireless image download profile TFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode tftp
Device(config-wireless-image-download-profile-tftp)# tftp-image-server 10.1.1.1
```

tftp-path

To configure the path at the TFTP server for trace log export, use the **tftp-path** command. Use the **no** form of the command to negate the command or to set the command to its default.

`tftp-path`*tftp-path*

`no tftp-path`*tftp-path*

Syntax Description

tftp-path	Specifies the path at the TFTP server.

Command Default

None

Command Modes

Wireless trace export profile TFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode tftp
Device(config-wireless-trace-export-profile-tftp)# tftp-path
/download/object/stream/images/ap-images
```

tftp-server

To configure the TFTP server address for trace export, use the **tftp-server** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
tftp-server {A.B.C.D | X:X:X:X::X}

no tftp-server {A.B.C.D | X:X:X:X::X}
```

Syntax Description

A.B.C.D	Specifies the TFTP IPv4 server address.
X:X:X:X::X	Specifies the TFTP IPv6 server address.

Command Default

None

Command Modes

Wireless trace export profile TFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode tftp
Device(config-wireless-trace-export-profile-tftp)# tftp-server 10.1.1.1
```

udp-timeout

To configure timeout value for UDP sessions, use the **udp-timeout** command.

udp-timeout *timeout_value*

Syntax Description

timeout_value	Is the timeout value for UDP sessions. The range is from 1 to 30 seconds. **Note** The *public-key* and *resolver* parameter-map options are automatically populated with the default values. So, you need not change them.

Command Default

None

Command Modes

Profile configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to configure timeout value for UDP sessions:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type umbrella global
Device(config-profile)# token 57CC80106C087FB1B2A7BAB4F2F4373C00247166
Device(config-profile)# local-domain dns_wl
Device(config-profile)# udp-timeout 2
Device(config-profile)# end
```

umbrella-param-map

To configure the Umbrella OpenDNS feature for WLAN, use the **umbrella-param-map** command.

umbrella-param-map *umbrella-name*

Syntax Description

umbrella-name

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to configure the Umbrella OpenDNS feature for WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# umbrella-param-map global
Device(config-wireless-policy)# end
```

update-timer

To configure the mDNS update timers for flex profile, use the **update-timer** command. To disable the command, use the **no** form of this command.

update-timer { **service-cache** *<1-100>* | **statistics** *<1-100>* }

update-timer { **service-cache** *<1-100>* | **statistics** *<1-100>* }

Syntax Description

update-timer	Configures the mDNS update timers for flex profile.
service-cache *<1-100>*	Specifies the mDNS update service-cache timer for flex profile. The default value is one minute,
statistics *<1-100>*	Specifies the mDNS update statistics timer for flex profile. The default value is one minute,

Command Default

None

Command Modes

mDNS flex profile configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to configure the mDNS update timers for flex profile:

```
Device(config-mdns-flex-prof)# update-timer service-cache 20
```

urlfilter list

To configure Flex URL filtering commands for ACL binding, use the **urlfilter list** c in the wireless flex profile ACL mode. To disable the feature, use the **no** form of the ommand.

urlfilter list *urlfilter-list-name*

[no] urlfilter list *urlfilter-list-name*

Syntax Description

urlfilter list	Configures the Flex URL filtering commands for ACL binding.
urlfilter-list-name	Specifies the URL filter list name.

Command Default

None

Command Modes

Wireless Flex Profile ACL configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1	This command was introduced.

Example

This example shows how the Flex URL filtering commands for ACL binding, is configured:

```
Device(config-wireless-flex-profile-acl)# urlfilter list urlfilter-list-name
```

username

To add a user who can access the Cisco ISE-3315 using SSH, use the **username** command in configuration mode. If the user already exists, the password, the privilege level, or both change with this command. To delete the user from the system, use the **no** form of this command.

[no] username *username* **password** {**hash** | **plain**} *password* **role** {**admin** | **user**] [**disabled** [**email** email-address]] [**email** email-address]

For an existing user, use the following command option:

username username **password role** {admin | **user**} password

Syntax Description

username	You should enter only one word which can include hyphen (-), underscore (_) and period (.). **Note** Only alphanumeric characters are allowed at an initial setup.
password	The command to use specify password and user role.
password	Password character length up to 40 alphanumeric characters. You must specify the password for all new users.
hash | plain	Type of password. Up to 34 alphanumeric characters.
role admin | user	Sets the privilege level for the user.
disabled	Disables the user according to the user's email address.
email *email-address*	The user's email address. For example, user1@example.com.
wlan-profile-name	Displays details of the WLAN profile.

Command Default

The initial user during setup.

Command Modes

Configuration

Usage Guidelines

The **username** command requires that the username and password keywords precede the hash | plain and the admin | user options.

Example 1

```
ncs/admin(config)# username admin password hash ###### role admin
ncs/admin(config)#
```

Example 2

```
ncs/admin(config)# username admin password plain Secr3tp@swd role admin
ncs/admin(config)#
```

Example 3

```
ncs/admin(config)# username admin password plain Secr3tp@swd role admin email
admin123@example.com
ncs/admin(config)#
```

violation

To configure stream violation policy on periodic reevaluation, use the **violation** command.

violation {**drop** | **fallback**}

Syntax Description

Parameter	Description
drop	Stream will be dropped on periodic reevaluation.
fallback	Stream will be demoted to BestEffort class on periodic reevaluation.

Command Default

None

Command Modes

config-media-stream

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure stream violation policy on periodic reevaluation:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# violation drop
```

wgb broadcast-tagging

To configure WGB broadcast tagging for a wireless policy profile, use the **wgb broadcast-tagging** command.

wgb broadcast-tagging

Command Default None

Command Modes config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to enable WGB broadcast tagging for a wireless policy profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy profile-policy-name
Device(config-wireless-policy)# wgb broadcast-tagging
```

wgb vlan

To configure WGB VLAN client support for a WLAN policy profile, use the **wgb vlan** command.

wgb vlan

Command Default None

Command Modes config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to enable WGB VLAN client support for the WLAN policy profile named *wlan1-policy-profile*:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy wlan1-policy-profile
Device(config-wireless-policy)# wgb vlan
```

whitelist acl

To configure the whitelist ACL, use the **whitelist acl** command.

whitelist acl {*standard_acl_value* | *extended_acl_value* | *acl_name*}

Syntax Description

standard_acl_value	Specifies the standard access list. Range is from 1 to 199.
extended_acl_value	Specifies the extended access list. Range is from 1300 to 2699.
acl_name	Specifies the named access list.

Command Default

None

Command Modes

ET-Analytics configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to enable in-active timer in the ET-Analytics configuration mode:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# et-analytics
Device(config-et-analytics)# whitelist acl
eta-whitelist
Device((config-et-analytics)# ip access-list
extended eta-whitelist
Device(config-ext-nacl)# permit udp any any eq tftp
Device(config-ext-nacl)# end
```

wired-vlan-range

To configure wired VLANs on which mDNS service discovery should take place, use the **wired-vlan-range** command. To disable the command, use the **no** form of this command.

wired-vlan-range *wired-vlan-range-value*

Syntax Description

wired-vlan-range	Configures wired VLANs on which mDNS service discovery should take place.
wired-vlan-range-value	Specifies the wired VLAN range value.

Command Default

None

Command Modes

mDNS flex profile configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to configure wired VLANs on which mDNS service discovery should take place:

```
Device(config-mdns-flex-prof)# wired-vlan-range range-value
```

config wlan assisted-roaming

To configure assisted roaming on a WLAN, use the **config wlan assisted-roaming** command.

config wlan assisted-roaming {**neighbor-list** | **dual-list** | **prediction**} {**enable** | **disable**} *wlan_id*

Syntax Description

neighbor-list	Configures an 802.11k neighbor list for a WLAN.
dual-list	Configures a dual band 802.11k neighbor list for a WLAN. The default is the band that the client is currently associated with.
prediction	Configures an assisted roaming optimization prediction for a WLAN.
enable	Enables the configuration on the WLAN.
disable	Disables the configuration on the WLAN.
wlan_id	Wireless LAN identifier between 1 and 512 (inclusive).

Command Default

The 802.11k neighbor list is enabled for all WLANs.

By default, dual band list is enabled if the neighbor list feature is enabled for the WLAN.

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

When you enable the assisted roaming prediction list, a warning appears and load balancing is disabled for the WLAN, if load balancing is already enabled on the WLAN.

The following example shows how to enable an 802.11k neighbor list for a WLAN:

```
(Cisco Controller) >config wlan assisted-roaming neighbor-list enable 1
```

wireless aaa policy

To configure a wireless AAA policy, use the **wireless aaa policy** command.

wireless aaa policy *aaa-policy*

Syntax Description

aaa-policy	Name of the wireless AAA policy.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure a wireless AAA policy named *aaa-policy-test*

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless aaa policy aaa-policy-test
```

wireless aaa policy

To configure a new AAA policy, use the **wireless aaa policy** command.

wireless aaa policy *aaa-policy-name*

Syntax Description

aaa-policy-name	AAA policy name.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure a AAA policy name:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless aaa policy my-aaa-policy
```

wireless autoqos policy-profile

To enable the **autoqos** wireless policy with an executable command, use the autoqos command. Use the **disable** command to disable wireless AutoQos.

wireless autoqos policy-profile*policy-profile-name* **default_policy_profile mode** { **clear** | **enterprise-avc** | **fastlane** | **guest** | **voice** }

wireless autoqos disable

Syntax Description

autoqos	Configures wireless Auto QoS.
mode	Specifies the wireless AutoQoS mode.
enterprise-avc	Enables AutoQos wireless enterprise AVC policy.
clear	Clears the configured wireless policy.
fastlane	Enables the AutoQos fastlane policy. This will disable and enable the 2.4GHz or 5GHz 802.11 network.
guest	Enables AutoQos wireless guest policy.
voice	Enables AutoQos wireless voice policy. This will disable and enable the 2.4GHz or 5GHz 802.11 network.

Command Default

None

Command Modes

Privilege EXEC mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

This example shows how to enable AutoQoS wireless enterprise policy:

```
Device# wireless autoqos policy-profile default-policy-profile mode enterprise-avc
```

wireless broadcast vlan

To enable broadcast support on a VLAN, use the **wireless broadcast vlan** command in global configuration mode. To disable Ethernet broadcast support, use the **no** form of the command.

wireless broadcast vlan [*vlan-id*]
no wireless broadcast vlan [*vlan-id*]

Syntax Description

vlan-id	(Optional) Specifies the VLAN ID to enable broadcast support to that VLAN. The value ranges from 1 to 4095.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

Use this command in the global configuration mode only.

This example shows how to enable broadcasting on VLAN 20:

```
Device(config)# wireless broadcast vlan 20
```

wireless client

To configure client parameters, use the **wireless client** command in global configuration mode.

wireless client {**association limit** *assoc-number* **interval** *interval* | **band-select** {**client-rssi** *rssi* | **cycle-count** *count* | **cycle-threshold** *threshold* | **expire dual-band** *timeout* | **expire suppression** *timeout*} | **max-user-login** *max-user-login* | **timers auth-timeout** *seconds* | **user-timeout** *user-timeout*}

Syntax Description

association limit *assoc-number* **interval** *interval*	Enables association request limit per access point slot at a given interval and configures the association request limit interval. You can configure number of association request per access point slot at a given interval from one through 100. You can configure client association request limit interval from 100 through 10000 milliseconds.
band-select	Configures the band select options for the client.
client-rssi *rssi*	Sets the client received signal strength indicator (RSSI) threshold for band select. The minimum dBm of a client RSSI to respond to probe is between -90 and -20.
cycle-count *count*	Sets the band select probe cycle count. You can configure the cycle count from 1 to 10.
cycle-threshold *threshold*	Sets the time threshold for a new scanning cycle. You can configure the cycle threshold from 1 to 1000 milliseconds.
expire dual-band *timeout*	Sets the timeout before stopping to try to push a given client to the 5-GHz band. You can configure the timeout from 10 to 300 seconds, and the default value is 60 seconds.
expire suppression *timeout*	Sets the expiration time for pruning previously known dual-band clients. You can configure the suppression from 10 to 200 seconds, and the default timeout value is 20 seconds.
max-user-login *max-user-login*	Configures the maximum number of login sessions for a user.
timers auth-timeout *seconds*	Configures the client timers.
user-timeout *user-timeout*	Configures the idle client timeout.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to set the proble cycle count for band select to 8:

```
Device# configure terminal
Device(config)# wireless client band-select cycle-count 8
Device(config)# end
```

This example shows how to set the time threshold for a new scanning cycle with threshold value of 700 milliseconds:

```
Device# configure terminal
Device(config)# wireless client band-select cycle-threshold 700
Device(config)# end
```

This example shows how to suppress dual-band clients from the dual-band database after 70 seconds:

```
Device# configure terminal
Device(config)# wireless client band-select expire suppression 70
Device(config)# end
```

wireless client mac-address

To configure the wireless client settings, use the **wireless client mac-address** command in global configuration mode.

wireless client mac-address *mac-addr* **ccx** {**clear-reports** | **clear-results** | **default-gw-ping** | **dhcp-test** | **dns-ping** | **dns-resolve hostname** *host-name* | **get-client-capability** | **get-manufacturer-info** | **get-operating-parameters** | **get-profiles** | **log-request** {**roam** | **rsna** | **syslog**} | **send-message** *message-id* | **stats-request** *measurement-duration* {**dot11** | **security**} | **test-abort** | **test-association** *ssid bssid dot11 channel* | **test-dot1x** [*profile-id*] *bssid dot11 channel* | **test-profile** {**any***profile-id*}}

Syntax Description

mac-addr	MAC address of the client.
ccx	Cisco client extension (CCX).
clear-reports	Clears the client reporting information.
clear-results	Clears the test results on the controller.
default-gw-ping	Sends a request to the client to perform the default gateway ping test.
dhcp-test	Sends a request to the client to perform the DHCP test.
dns-ping	Sends a request to the client to perform the Domain Name System (DNS) server IP address ping test.
dns-resolve hostname *host-name*	Sends a request to the client to perform the Domain Name System (DNS) resolution test to the specified hostname.
get-client-capability	Sends a request to the client to send its capability information.
get-manufacturer-info	Sends a request to the client to send the manufacturer's information.
get-operating-parameters	Sends a request to the client to send its current operating parameters.
get-profiles	Sends a request to the client to send its profiles.
log-request	Configures a CCX log request for a specified client device.
roam	(Optional) Specifies the request to specify the client CCX roaming log
rsna	(Optional) Specifies the request to specify the client CCX RSNA log.
syslog	(Optional) Specifies the request to specify the client CCX system log.

send-message *message-id*

Sends a message to the client.

Message type that involves one of the following:

- 1—The SSID is invalid
- 2—The network settings are invalid.
- 3—There is a WLAN credibility mismatch.
- 4—The user credentials are incorrect.
- 5—Please call support.
- 6—The problem is resolved.
- 7—The problem has not been resolved.
- 8—Please try again later.
- 9—Please correct the indicated problem.
- 10—Troubleshooting is refused by the network.
- 11—Retrieving client reports.
- 12—Retrieving client logs.
- 13—Retrieval complete.
- 14—Beginning association test.
- 15—Beginning DHCP test.
- 16—Beginning network connectivity test.
- 17—Beginning DNS ping test.
- 18—Beginning name resolution test.
- 19—Beginning 802.1X authentication test.
- 20—Redirecting client to a specific profile.
- 21—Test complete.
- 22—Test passed.
- 23—Test failed.
- 24—Cancel diagnostic channel operation or select a WLAN profile to resume normal operation.
- 25—Log retrieval refused by the client.
- 26—Client report retrieval refused by the client.
- 27—Test request refused by the client.
- 28—Invalid network (IP) setting.
- 29—There is a known outage or problem with the network.

- 30—Scheduled maintenance period.
- 31—The WLAN security method is not correct.
- 32—The WLAN encryption method is not correct.
- 33—The WLAN authentication method is not correct.

stats-request *measurement-duration*	Senda a request for statistics.
dot11	Optional) Specifies dot11 counters.
security	(Optional) Specifies security counters.
test-abort	Sends a request to the client to abort the current test.
test-association *ssid bssid dot11 channel*	Sends a request to the client to perform the association test.
test-dot1x	Sends a request to the client to perform the 802.1x test.
profile-id	(Optional) Test profile name.
bssid	Basic SSID.
dot11	Specifies the 802.11a, 802.11b, or 802.11g network.
channel	Channel number.
test-profile	Sends a request to the client to perform the profile redirect test.
any	Sends a request to the client to perform the profile redirect test.
profile-id	Test profile name. **Note** The profile ID should be from one of the client profiles for which client reporting is enabled.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

The **default-gw-ping** test does not require the client to use the diagnostic channel.

This example shows how to clear the reporting information of the client MAC address 00:1f:ca:cf:b6:60:

```
Device# configure terminal
```

```
Device(config)# wireless client mac-address 00:1f:ca:cf:b6:60 ccx clear-reports
Device(config)# end
```

wireless config validate

To validate whether the wireless configuration is complete and consistent (all the functional profiles and tags are defined, and all the associations are complete and consistent), use the **wireless config validate** command in privileged EXEC mode.

wireless config validate

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

In Cisco vEWLC, the wireless configuration is built using a collection of profiles, with each profile defining a functional block. These functional blocks are defined independently and is used to realize well-defined associations through intent based work-flows in building the wireless LAN. Such flexibility of modularizing the functional blocks requires the administrator to ensure that all associations are consistent and complete.

To ensure completeness and consistency of the wireless configuration, a configuration validation library is used to validate the configuration definitions across tables. The **wireless config validate** exec command is introduced from this release to validate the wireless configuration and report inconsistencies, if any, using contextual error message that is visible in btrace infra and on the console (if console logging is enabled). This command calls out any inconsistencies (unresolved associations) enabling you to realize a functional wireless LAN.

Use the following command to direct the output to a file: **show logging | redirect bootflash:** *filename* .

The following set of wireless configurations are validated:

RF tag	Site tag	Policy tag	Policy profile	Flex profile
site-tag	flex-profile	wlan profile	IPv4 ACL name	VLAN ACL
poliy-tag	ap-profile	policy profile	Fabric name	ACL-policy
rf-tag	-—	-—	service-policy input and output name	RF Policy (5GHz and 24GHz)
-—	-—	-—	service-policy input and client output name	-—

Example

The following is sample output from the **wireless config validate** command

```
Device# wireless config validate

Oct 10 18:21:59.576 IST: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0: wncmgrd:
 Error in AP: fc99.473e.0a90  Applied site-tag : mysite definitiondoes not exist
Oct 10 18:21:59.576 IST: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0: wncmgrd:
 Error in AP: fc99.473e.0a90  Applied policy-tag : mypolicy definition does not exist
Oct 10 18:21:59.576 IST: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0: wncmgrd:
 Error in AP: fc99.473e.0a90  Applied rf-tag : myrf definition does not exist
```

wireless country

To configure one or more country codes for a device, use the **wireless country** command.

wireless country *country-code*

Syntax Description

country-code	Two-letter country code.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Usage Guidelines

The Cisco must be installed by a network administrator or qualified IT professional and the installer must select the proper country code. Following installation, access to the unit should be password protected by the installer to maintain compliance with regulatory requirements and to ensure proper unit functionality. See the related product guide for the most recent country codes and regulatory domains.

This example shows how to configure country code on the device to IN (India):

```
Device(config)# wireless country IN
```

wireless exclusionlist mac address

To manually add clients to the exclusionlist, use the wireless exclusion list command. To remove the manual entry, use the no form of the command.

wireless exclusionlist *mac_address* **description**

Syntax Description

description *value*	Configures the entry description.

Command Default

None

Command Modes

Global Configuration

Command History

Cisco IOS XE Gibraltar 16.10.1	Modification
	This command was introduced in this release.

Usage Guidelines

If a client was added to the exclusion list dynamically, the command to remove it is **wireless client mac-address xxxx.xxxx.xxxx deauthenticate** from enable mode.

Example

This example shows how to manage exclusion entries:

```
Device(config)# wireless exclusion list xxxx.xxxx.xxxx
```

wireless ipv6 ra wired

To enable the forwarding of Router Advertisement message to the wired clients, use the **wireless ipv6 ra wired** command.

wireless ipv6 ra wired { **nd** { **na-forward** | **ns-forward** } | **ra-wired** }

Syntax Description

nd	Configures wireless IPv6 ND parameters.
na-forward	Enables forwarding of Neighbor Advertisement to wireless clients.
ns-forward	Enable forwarding of Neighbor Solicitation to wireless clients.
ra	Configures wireless IPv6 Router Advertisement parameters.
wired	Enables forwarding of Router Advertisement message to the wired clients.

Command Default

None

Command Modes

Global Configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.3	This command was introduced.

Example

The following example shows how to enable the forwarding of Router Advertisement message to the wired clients:

```
Device(config)# wireless ipv6 ra wired
```

Warning The **wireless ipv6 ra wired** command must be enabled only for certification purpose and not during the deployment.

wireless load-balancing

To globally configure aggressive load balancing on the controller, use the **wireless load-balancing** command in global configuration mode.

wireless load-balancing {**denial** *denial-count* | **window** *client-count*}

Syntax Description

denial *denial-count*	Specifies the number of association denials during load balancing. Maximum number of association denials during load balancing is from 1 to 10 and the default value is 3.
window *client-count*	Specifies the aggressive load balancing client window, with the number of clients needed to trigger aggressive load balancing on a given access point. Aggressive load balancing client window with the number of clients is from 0 to 20 and the default value is 5.

Command Default

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

Load-balancing-enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.

When you use Cisco 7921 and 7920 Wireless IP Phones with controllers, make sure that aggressive load balancing is disabled on the voice WLANs for each controller. Otherwise, the initial roam attempt by the phone might fail, causing a disruption in the audio path.

This example shows how to configure association denials during load balancing:

```
Device# configure terminal
Device(config)# wireless load-balancing denial 5
Device(config)# end
```

wireless macro-micro steering transition-threshold

To configure micro-macro transition thresholds, use the **wireless macro-micro steering transition-threshold** command.

wireless macro-micro steering transition-threshold {**balancing-window** | **client count** *number-clients* }{**macro-to-micro** | **micro-to-macro** *RSSI in dBm*}

Syntax Description

balancing-window	Active instance of the configuration in Route-processor slot 0.
client	Standby instance of the configuration in Route-processor slot 0.
number-clients	Valid range is 0 to 65535 clients.
macro-to-micro	Configures the macro to micro transition RSSI.
micro-to-macro	Configures micro-macro client load balancing window.
RSSI in dBm	RSSI in dBm. Valid range is –128 to 0.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure balancing-window:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless macro-micro steering transition-threshold balancing-window
number-of-clients
```

wireless macro-micro steering probe-suppression

To configure micro-macro probe suppressions, use the **wireless macro-micro steering probe-suppression** command.

wireless macro-micro steering probe-suppression {**aggressiveness** *number-of-cycles* | | **hysteresis***RSSI in dBm* | **probe-auth** | **probe-only**}

Syntax Description

aggressiveness	Configures probe cycles to be suppressed. The number of cycles range between 0 - 255.
hysteresis	Indicate show much greater the signal strength of a neighboring access point must be in order for the client to roam to it. The RSSI decibel value ranges from -6 to -3.
probe-auth	Enables mode to suppress probes and single auth
probe-only	Enables mode to suppress only probes

Command Default

None

Command Modes

Global configuration (config)

Command History

Examples

The following example shows how to configure balancing-window:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless macro-micro steering probe-suppression aggressiveness
number-of-cycles
```

wireless management certificate

To create a wireless management certificate details, use the **wireless management certificate** command.

wireless management certificate ssc {**auth-token** {**0** | **8**} *token* | **trust-hash** *hash-key* }

Syntax Description

auth-token	Authentication token.
token	Token name.
trust-hash	Trusted SSC hash list.
hash-key	SHA1 fingerprint.
0	Specifies an UNENCRYPTED token.
8	Specifies an AES encrypted token.

Command Default

None

Command Modes

Global Configuration(config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Example

The following example shows how to configure a wireless management certificate:

```
Device# configure terminal
Device(config)# wireless management certificate ssc trust-hash test
```

wireless management interface

To create a wireless management interface, use the **wireless management interface** command.

wireless management interface { **GigabitEthernet** | **Loopback** | **Vlan** } *interface-number*

Syntax Description

interface-number	Interface number.

Command Default

None

Command Modes

Global Configuration(config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Example

The following example shows how to configure a wireless management interface:

```
Device# configure terminal
Device(config)# wireless management interface vlan vlan1
```

wireless management trustpoint

To create a wireless management trustpoint, use the **wireless management trustpoint** command.

wireless management trustpoint *trustpoint-name*

Syntax Description

trustpoint-name	Trustpoint name.

Command Default

None

Command Modes

Global Configuration(config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

Use this command only on the Cisco Catalyst 9800 Wireless Controller for Cloud platform and not on appliances as the appliances use the SUDI certificate by default without the need for this command.

Example

The following example shows how to configure a wireless management trustpoint:

```
Device# configure terminal
Device(config)# wireless management trustpoint test
```

wireless ewc-ap ap ap-type

To convert a single AP to CAPWAP or to embedded wireless controller, use the **wireless ewc-ap ap ap-type** command.

wireless ewc-ap ap ap-type *Cisco-AP-name* { **capwap** | **ewc** }

Syntax Description

ewc-ap	Configures the embedded wireless controller parameters.
ap-type	Configures the AP parameter.
Cisco-AP-name	Indicates the name of the Cisco AP.
capwap	Changes to Capwap ap-type.
ewc	Changes to the embedded wireless controller ap-type.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This message was introduced.

Example

The following example shows how to convert a single AP to a CAPWAP ap-type or a embedded wireless controller ap-type:

```
Device#wireless ewc-ap ap ap-type ap_name {capwap | ewc}
```

wireless ewc-ap ap capwap

To specify the CAPWAP parameters for an AP, use the **wireless ewc-ap ap capwap** command.

wireless ewc-ap ap capwap *Primary-Controller-Name* { **A.B.C.D** | **X:X:X:X::X** }

Syntax Description

ewc-ap	Configures the embedded wireless controller parameters.
capwap	Configures the CAPWAP parameters.
Primay-Controller-Name	Indicates the name of the controller.
A.B.C.D	Indicates the IPv4 address of the primary controller.
X:X:X:X::X	Indicates the IPv6 address of the primary controller.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE 16.12.1	This message was introduced.

Example

The following example shows how to specify the CAPWAP parameters for an AP:

```
Device#wireless ewc-ap ap capwap controller_name {10.1.1.1 | 9:0:0:0::1}
```

wireless ewc-ap ap reload

To reload the embedded wireless controller AP, use the **wireless ewc-ap ap reload** command.

wireless ewc-ap ap reload

Syntax Description

ewc-ap	Configures the embedded wireless controller parameters.
reload	Reloads the embedded wireless controller AP.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE 16.12.1	This message was introduced.

Example

The following example shows how to reload the embedded wireless controller AP:

```
Device#wireless ewc-ap ap reload
```

wireless ewc-ap ap shell

To access the AP parameters on the embedded wireless controller AP shell, use the **wireless ewc-ap ap shell** command.

wireless ewc-ap ap shell { **chassis** { *chassis-number* | **active** | **standby** } **R0** | **username** }

Syntax Description

chassis	Specifies the chassis.
chassis-number	Specifies the chassis number as either 1 or 2.
active	Configures the active instance in route processor slot 0.
standby	Configures the standby instance in route processor slot 0.
R0	Specifies the route processor in slot 0.
username	Specifies the AP management username.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device#wireless ewc-ap ap shell chassis 1 R0
```

wireless ewc-ap ap shell username

To configure the AP management username on the embedded wireless controller AP shell, use the **wireless ewc-ap ap shell username** command.

wireless ewc-ap ap shell username *username* **chassis** { *chassis-number* | **active** | **standby** } **R0**

Syntax Description

chassis	Specifies the chassis.
chassis-number	Specifies the chassis number as either 1 or 2.
active	Configures the active instance in route processor slot 0.
standby	Configures the standby instance in route processor slot 0.
R0	Specifies the route processor in slot 0.
username	Specifies the AP management username.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device#wireless ewc-ap ap shell username username1 chassis 1 R0
```

wireless ewc-ap preferred-master

To select the standby controller when the network is up and running, use the **wireless ewc-ap preferred-master** command.

wireless ewc-ap preferred-master *AP-name*

Syntax Description

ewc-ap	Configures the embedded wireless controller parameters.
preferred-master	Configures the preferred primary AP.
AP-name	Indicates the name of the preferred primary AP.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This message was introduced.

Example

The following example shows how to set a preferred primary ap-type:

```
Device(config)#wireless ewc-ap preferred-master AP-name
```

wireless ewc-ap factory-reset

To perform factory reset on the embedded wireless controller and on all the access points connected to the controller, use the **wireless ewc-ap factory-reset** command.

wireless ewc-ap factory-reset

Syntax Description

ewc-ap	Configures the embedded wireless controller parameters .
factory-reset	Resets Cisco AP configuration to factory default.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Example

The following example shows how to factory-reset the embedded wireless controller network:

```
Device#wireless ewc-ap factory-reset
```

wireless ewc-ap vrrp vrid

To configure the embedded wireless controller VRRP network identifier, use the **wireless ewc-ap vrrp vrid** command.

wireless ewc-ap vrrp vrid*value <1-255>*

Syntax Description

ewc-ap	Configures the embedded wireless controller parameters.
vrrp	Configires the preferred primary APembedded wireless controller VRRP.
vrid	Indicates the VRRP VRID. Values are from 1-255. The default value is 1.
value	Indicates the VRRP VRID value.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This message was introduced.

Example

The following example shows how to configure the VRRP network identifier:

```
Device#wireless ewc-ap vrrp vrid 1
```

wireless profile flex

To configures a wireless flex profile and enter wireless flex profile configuration mode, use the **wireless profile flex** command. To disable the feature, use the **no** form of the command.

wireless profile flex *custom-flex-profile*

[no] wireless profile flex *custom-flex-profile*

Syntax Description

wireless profile flex	Configures a wireless flex profile and enter wireless flex profile configuration mode.
custom-flex-profile	Specifies the flex profile name.

Command Default

None

Command Modes

Wireless flex profile mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

Example

This examples shows how the wireless flex profile is configured:

```
Device(config)#wireless profile flex custom-flex-profile
```

wireless profile image-download default

To configure the default image download profile for AP Join Download and Predownload, use the following command:

Note **Default** is the only profile name that you can enter.

wireless profile image-download default

Syntax Description

wireless profile	Configures the wireless profile parameters.
image-download	Configures the EWC-AP image download parameters.
default	Specifies the profile name - default. Default is the only profile name that you can enter.

Command Default None

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device# wireless profile image-download default
```

wireless profile policy

To configure WLAN policy profile, use the **wireless profile policy** command.

wireless profile policy *policy-profile*

Syntax Description

policy-profile	Name of the WLAN policy profile.

Command Default

The default profile name is default-policy-profile.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure a WLAN policy profile:

```
Device(config)# wireless profile policy mywlan-profile-policy
```

wireless profile transfer

To configure the export of trace logs on the embedded wireless controller, use the **wireless profile transfer** command. Use the **no** form of this command to negate the command or to set the command to its default.

[**no**] **wireless profiletransfertrace-export** *trace-export-profile-name*

Syntax Description

trace-export	Configures the trace export parameters.
trace-export-profile-name	Specifies the trace export profile name.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device# wireless profile transfer trace-export trace-export-profile-name
```

wireless rfid

To set the static radio-frequency identification (RFID) tag data timeout value, use the **wireless rfid** command in global configuration mode.

wireless rfid timeout *timeout-value*

Syntax Description

timeout	Configures the static RFID tag data timeout value.
timeout-value	RFID tag data timeout value. Valid values range from 60-7200.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to set the static RFID tag data timeout value.

```
Device(config)# wireless rfid timeout 70
```

wireless security dot1x

To configure IEEE 802.1x global configurations, use the **wireless security dot1x** command.

wireless security dot1x [{**eapol-key** {**retries** *retries* | **timeout** *milliseconds*} | **group-key interval** *sec* | **identity-request** {**retries** *retries* | **timeout** *seconds*} | **radius** [**call-station-id**] {**ap-macaddress** | **ap-macaddress-ssid** | **ipaddress** | **macaddress**} | **request** {**retries** *retries* | **timeout** *seconds*} | **wep key** {**index 0** | **index 3**}}]

Syntax Description

eapol-key	Configures eapol-key related parameters.
retries *retries*	(Optional) Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client. The default value is 2.
timeout *milliseconds*	(Optional) Specifies the amount of time (200 to 5000 milliseconds) that the controller waits before retransmitting an EAPOL (WPA) key message to a wireless client using EAP or WPA/WPA-2 PSK. The default value is 1000 milliseconds.
group-key interval *sec*	Configures EAP-broadcast key renew interval time in seconds (120 to 86400 seconds).
identity-request	Configures EAP ID request related parameters.
retries *retries*	(Optional) Specifies the maximum number of times (0 to 4 retries) that the controller request the EAP ID. The default value is 2.
timeout *seconds*	(Optional) Specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting an EAP Identity Request message to a wireless client. The default value is 30 seconds.
radius	Configures radius messages.
call-station-id	(Optional) Configures Call-Station Id sent in radius messages.
ap-macaddress	Sets Call Station Id Type to the AP's MAC Address.
ap-macaddress-ssid	Sets Call Station Id Type to 'AP MAC address':'SSID'.
ipaddress	Sets Call Station Id Type to the system's IP Address.
macaddress	Sets Call Station Id Type to the system's MAC Address.
request	Configures EAP request related parameters.

retries *retries*	(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the maximum number of times (0 to 20 retries) that the controller retransmits the message to a wireless client. The default value is 2.
timeout *seconds*	(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting the message to a wireless client. The default value is 30 seconds.
wep key	Configures 802.1x WEP related paramters.
index 0	Specifies the WEP key index value as 0
index 3	Specifies the WEP key index value as 3

Command Default

Default for eapol-key-timeout: 1 second.

Default for eapol-key-retries: 2 retries.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None.

This example lists all the commands under **wireless security dot1x** .

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless security dot1x ?
  eapol-key         Configure eapol-key related parameters
  group-key         Configures EAP-broadcast key renew interval time in seconds
  identity-request  Configure EAP ID request related parameters
  radius            Configure radius messages
  request           Configure EAP request related parameters
  wep               Configure 802.1x WEP related paramters
  <cr>
```

wireless security dot1x radius accounting mac-delimiter

To configure a MAC delimiter for called-station-ID or a calling-station-ID, use the **wireless security dot1x radius accounting mac-delimiter** command.

To remove MAC delimiter for a called-station-ID or a calling-station-ID, use the **no** form of the command.

wireless security dot1x radius accounting mac-delimiter {**colon** | **hyphen** | **none** | **single-hyphen** }

Syntax Description

colon	Sets the delimiter to colon.
hyphen	Sets the delimiter to hyphen.
none	Disables delimiters.
single-hyphen	Sets the delimiters to single hyphen.

Command Default

None

Command Modes

Global Configuration Mode

Command History

Release	Modification
Cisco IOS XE 3.6.0 E	This command was introduced.

This example shows how to configure a MAC delimiter for called-station-ID or a calling-station-ID to colon:

```
Device(config)# wireless security dot1x radius accounting mac-delimiter colon
```

wireless security dot1x radius accounting username-delimiter

To set the delimiter type, use **wireless security dot1x radius accounting username-delimiter** command, to remove the configuration, use the **no** form of this command.

wireless security dot1x radius accounting username-delimiter {**colon | hyphen | none | single-hyphen**}

Syntax Description

colon	Sets the delimiter to colon.
hyphen	Sets the delimiter to hyphen.
none	Disables delimiters.
single-hyphen	Sets the delimiters to single hyphen.

Command Default

None

Command Modes

Global Configuration Mode.

Command History

Release	Modification
Cisco IOS XE 3.7.2 E	This command was introduced.

This example shows how to sets the delimiter to colon.

```
Device(config)# wireless security dot1x radius acounting username-delimiter colon
```

wireless security dot1x radius callStationIdCase

To configure Call Station Id CASE send in RADIUS messages, use the **wireless security dot1x radius callStationIdCase** command.

To remove the Call Station Id CASE send in RADIUS messages, use the **no** form of the command.

wireless security dot1x radius callStationIdCase {**lower** | **upper**}

Syntax Description

lower	Sends all Call Station Ids to RADIUS in lowercase
upper	Sends all Call Station Ids to RADIUS in uppercase

Command Default

None

Command Modes

Global Configuration Mode

Command History

Release	Modification
Cisco IOS XE 3.6.0 E	This command was introduced.

This example shows how to configure Call Station Id CASE send in RADIUS messages in lowercase:

```
Device(config)# wireless security dot1x radius callstationIdCase lower
```

wireless security dot1x radius mac-authentication call-station-id

To configure call station ID type for mac-authentication, use the **wireless security dot1x radius mac-authentication call-station-id** command. To remove the configuration, use the **no** form of it.

wireless security dot1x radius mac-authentication call-station-id ap-ethmac-only | ap-ethmac-ssid | ap-group-name | ap-label-address | ap-label-address-ssid | ap-location | ap-macaddress | ap-macaddress-ssid | ap-name | ap-name-ssid | ipaddress | macaddress | vlan-id

Syntax Description

ap-ethmac-only	Sets call station ID type to the AP Ethernet MAC address.
ap-ethmac-ssid	Sets call station ID type to the format 'AP Ethernet MAC address':'SSID'.
ap-group-name	Sets call station ID type to the AP Group Name.
ap-label-address	Sets call station ID type to the AP MAC address on AP Label.
ap-label-address-ssid	Sets call station ID type to the format 'AP Label MAC address': 'SSID'.
ap-location	Sets call station ID type to the AP Location.
ap-macaddress	Sets call station ID type to the AP Radio MAC Address.
ap-macaddress-ssid	Sets call station ID type to the 'AP radio MAC Address':'SSID'.
ap-name	Sets call station ID type to the AP name.
ap-name-ssid	Sets call station ID type to the format 'AP name':'SSID'.
ipaddress	Sets call station ID type to the system IP Address.
macaddress	Sets call station ID type to the system MAC Address.
vlan-id	Sets call station ID type to the VLAN ID.

Command Default

None

Command Modes

Global Configuration Mode

Command History

Release	Modification
Cisco IOS XE 3.7.2 E	This command was introduced.

The example show how to set call station ID type to the AP Ethernet MAC address:

```
Device(config)# wireless security dot1x radius mac-authentication call-station-id
ap-ethmac-only
```

wireless security dot1x radius mac-authentication mac-delimiter

To configure MAC-Authentication attributes, use the **wireless security dot1x radius mac-authentication mac-delimiter** command.

To remove MAC-Authentication attributes, use the **no** form of the command.

wireless security dot1x radius mac-authentication mac-delimiter {**colon** | **hyphen** | **none** | **single-hyphen** }

Syntax Description

colon	Sets the delimiter to colon.
hyphen	Sets the delimiter to hyphen.
none	Disables delimiters.
single-hyphen	Sets the delimiters to single hyphen.

Command Default

None

Command Modes

Global Configuration Mode

Command History

Release	Modification
Cisco IOS XE 3.6.0 E	This command was introduced.

This example shows how to configure MAC-Authentication attributes to colon:

```
Device(config)# Scurity dot1x radius mac-authentication mac-delimiter colon
```

wireless security web-auth retries

To enable web authentication retry on a particular WLAN, use the **wireless wireless security web-auth retries** command. To disable, use the **no** form of the command.

wireless securityweb-authretries*retries*
nowireless securityweb-authretries

Syntax Description

wireless security web-auth	Enables web authentication on a particular WLAN.
retries *retries*	Specifies maximum number of web authentication request retries. The range is from 0 through 30. The default value is 3.

Command Default

Command Modes

config

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None.

This example shows how to enable web authentication retry on a particular WLAN.

```
Device#configure terminal
Device# wireless security web-auth retries 10
```

wireless tag policy

To configure wireless tag policy, use the **wireless tag policy** command.

wireless tag policy *policy-tag*

Syntax Description

policy-tag	Name of the wireless tag policy.

Command Default

The default policy tag is default-policy-tag.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure a wireless policy tag:

```
Device(config)# wireless tag policy guest-policy
```

wireless tag site

To configure a wireless site tag, use the **wireless tag site** *site-tag*command.

wireless tag site *site-tag*

Syntax Description

site-tag	Name of the site tag.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to configure a site tag:

```
Device(config)# wireless tag site test-site
```

wireless wps ap-authentication threshold

To configure the alarm trigger threshold for access point neighbor authentication, use the **wireless wps ap-authentication threshold** command. To remove the access point neighbor authentication, use the no form of the command.

wireless wps ap-authentication threshold *value*

no wireless wps ap-authentication threshold *value*

Syntax Description

threshold *value*	Specifies that the WMM-enabled clients are on the wireless LAN. The threshold value range is between 1 and 255. The default value is 1.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to configure the alarm trigger threshold for access point neighbor authentication:

```
Device(config)# wireless wps ap-authentication threshold 1
```

wireless wps client-exclusion

To configure client exclusion policies, use the **wireless wps client-exclusion** command. To remove the client exclusion policies, use the **no** form of the command.

wireless wps client-exclusion {**all** | **dot11-assoc** | **dot11-auth** | **dot1x-auth** | **ip-theft** | **web-auth**}
no wireless wps client-exclusion {**all** | **dot11-assoc** | **dot11-auth** | **dot1x-auth** | **ip-theft** | **web-auth**}

Syntax Description

dot11-assoc	Specifies that the controller excludes clients on the sixth 802.11 association attempt, after five consecutive failures.
dot11-auth	Specifies that the controller excludes clients on the sixth 802.11 authentication attempt, after five consecutive failures.
dot1x-auth	Specifies that the controller excludes clients on the sixth 802.11X authentication attempt, after five consecutive failures.
ip-theft	Specifies that the control excludes clients if the IP address is already assigned to another device. For more information, see the Usage Guidelines section.
web-auth	Specifies that the controller excludes clients on the fourth web authentication attempt, after three consecutive failures.
all	Specifies that the controller excludes clients for all of the above reasons.

Command Default

Enabled.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

In IP-theft scenarios, there are differences between the older Cisco IOS XE releases and the Cisco IOS XE Denali 16.x releases:

Older Cisco IOS XE Releases	Cisco IOS XE Denali 16.x Releases
Priority wise, wired clients have higher priority over wireless clients, and DHCP IP has higher priority over static IP. The client security type is not checked; security of all client types are treated with same priority. If the existing binding is from a higher priority source, the new binding is ignored and an IP-theft is signaled. If the existing binding has the same source-priority as the new binding, the binding is ignored and an IP-theft is signaled. This ensures that the bindings are not toggled if two hosts send traffic using the same IP. Only the initial binding is retained in the software. If the new binding is from a higher priority source, the existing binding is replaced. This results in an IP-theft notification of existing binding and also a new binding notification.	There is not really a fundamental difference between wired and wireless; what matters is the trust (preflevel) of the entry, which is a function on how it was learnt (ARP, DHCP, ND, and so on) and the policy that is attached to the port. When preflevel is equal, the IP takeover is denied if the old entry is still reachable. IP takeover occurs when the update comes from a trusted port or a new entry gets IP from the DHCP server. Otherwise, you must explicitly grant it. The IP-theft is not reported if an old entry is replaced by a new and a more trusted one.

This example shows how to disable clients on the 802.11 association attempt after five consecutive failures.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless wps client-exclusion dot11-assoc
```

wireless wps mfp ap-impersonation

To configure AP impersonation detection, use the **wireless wps mfp ap-impersonation** command. Use the **no** form of this command to disable the configuration.

wireless wps mfp ap-impersonation

no wireless wps mfp ap-impersonation

Syntax Description

ap-impersonation	Configures AP impersonation detection.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to configure AP impersonation detection:

```
Device(config)# wireless wps mfp ap-impersonation
```

wireless wps rogue network-assurance enable

To enable the rogue wireless service assurance (WSA) events, use the **wireless wps rogue network-assurance enable** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue network-assurance enable

no wireless wps rogue network-assurance enable

Syntax Description

network-assurance enable	Enables rogue WSA events.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to enable the rogue wireless service assurance events:

```
Device(config)# wireless wps rogue network-assurance enable
```

wireless wps rogue ap aaa

To configure the use of AAA/local database to detect valid AP MAC addresses, use the **wireless wps rogue ap aaa** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap aaa

no wireless wps rogue ap aaa

Syntax Description

aaa	Configures the use of AAA or local database to detect valid AP MAC addresses.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to configure the use of AAA/local database to detect valid AP MAC addresses:

```
Device(config)# wireless wps rogue ap aaa
```

wireless wps rogue ap aaa polling-interval

To configures Rogue AP AAA validation interval, in seconds, use the **wireless wps rogue ap aaa polling-interval** command. To disable the configuration, use the no form of this command.

wireless wps rogue ap aaa polling-interval *60 - 86400*

no wireless wps rogue ap aaa polling-interval *60 - 86400*

Syntax Description

aaa	Sets the use of AAA or local database to detect valid AP MAC addresses.
polling-interval	Configures the rogue AP AAA validation interval.
60 - 86400	Specifies AP AAA validation interval, in seconds.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None

Example

This example shows how to configures Rogue AP AAA validation interval, in seconds:

```
Device(config)# wireless wps rogue ap aaa polling-interval 120
```

wireless wps rogue ap init-timer

To configure the init timer for rogue APs, use the **wireless wps rogue ap init-timer** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap init-timer

no wireless wps rogue ap init-timer

Syntax Description

init-timer	Configures the init timer for rogue APs.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to configure the init timer for rogue APs:

```
Device(config)# wireless wps rogue ap init-timer
```

wireless wps rogue ap mac-address rldp initiate

To initiate and configure Rogue Location Discovery Protocol on rogue APs, use the **wireless wps rogue ap mac-address rldp initiate** command.

wireless wps rogue ap mac-address <*MAC Address*> **rldp initiate**

Syntax Description

wps	Configures the WPS settings.
rogue	Configures the global rogue devices.
ap mac-address <*MAC Address*>	The MAC address of the APs.
rldp initiate	Initiates RLDP on rogue APs.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to initiate and configure Rogue Location Discovery Protocol on rogue APs:

```
Device# wireless wps rogue ap mac-address 10.1.1 rldp initiate
```

wireless wps rogue ap notify-min-rssi

To configure the minimum RSSI notification threshold for rogue APs, use the **wireless wps rogue ap notify-min-rssi** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap notify-min-rssi

no wireless wps rogue ap notify-min-rssi

Syntax Description

notify-min-rssi	Configure the minimum RSSI notification threshold for rogue APs.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to configure the minimum RSSI notification threshold for rogue APs:

```
Device(config)# wireless wps rogue ap notify-min-rssi
```

wireless wps rogue ap notify-rssi-deviation

To configure the RSSI deviation notification threshold for rogue APs, use the **wireless wps rogue ap notify-rssi-deviation** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap notify-rssi-deviation

no wireless wps rogue ap notify-rssi-deviation

Syntax Description

notify-rssi-deviation	Configures the RSSI deviation notification threshold for rogue APs.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to configure the RSSI deviation notification threshold for rogue APs:

```
Device(config)# wireless wps rogue ap notify-rssi-deviation
```

wireless wps rogue ap rldp alarm-only

To set Rogue Location Discovery Protocol (RLDP) and alarm if rogue is detected, use the **wireless wps rogue ap rldp alarm-only** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap rldp alarm-only

no wireless wps rogue ap rldp alarm-only

Syntax Description

alarm-only	Sets RLDP and alarm if rogue is detected.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to set RLDP and alarm if rogue is detected:

```
Device(config)# wireless wps rogue ap rldp alarm-only
```

wireless wps rogue ap rldp alarm-only monitor-ap-only

To perform RLDP only on monitor APs, use the **wireless wps rogue ap rldp alarm-only monitor-ap-only** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap rldp alarm-only monitor-ap-only

no wireless wps rogue ap rldp alarm-only monitor-ap-only

Syntax Description

monitor-ap-only	Performs RLDP on monitor APs only.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to perform RLDP only on monitor APs,:

```
Device(config)# wireless wps rogue ap rldp alarm-only monitor-ap-only
```

wireless wps rogue ap rldp auto-contain

To configure RLDP, alarm and auto-contain if rogue is detected, use **wirelesswps rogueaprldp auto-contain** command. Use the **no** form of the command to disable the alarm.

[no] wireless wps rogue ap rldp auto-contain monitor-ap-only

Syntax Description

monitor-ap-only	Perform RLDP only on monitor AP

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Cisco IOS XE 3.7.3E	The **no** form of the command was introduced.

Example

This example shows how to configure an alarm for a detected rogue.

```
Device wireless wps rogue ap rldp auto-contain
```

wireless wps rogue ap rldp retries

To configure RLDP retry times on rogue APs, use the **wireless wps rogue ap rldp retries** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap rldp retries

no wireless wps rogue ap rldp retries

Syntax Description

retries	Configures RLDP retry times on rogue APs.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to configure RLDP retry times on rogue APs:

```
Device(config)# wireless wps rogue ap rldp retries
```

wireless wps rogue ap rldp schedule

To configure RLDP scheduling, use the **wireless wps rogue ap rldp schedule** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap rldp schedule

no wireless wps rogue ap rldp schedule

Syntax Description

schedule	Configures RLDP scheduling.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to configure RLDP scheduling:

```
Device(config)# wireless wps rogue ap rldp schedule
```

wireless wps rogue ap rldp schedule day

To configure the day when RLDP scheduling is to be done, use the **wireless wps rogue ap rldp schedule day** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap rldp schedule day { **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** } **start** *[HH:MM:SS]* **end** *[HH:MM:SS]*

no wireless wps rogue ap rldp schedule day { **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** } **start** *[HH:MM:SS]* **end** *[HH:MM:SS]*

Syntax Description

day {**friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday**}	Configures the day of the week when RLDP scheduling is to be done.
start *[HH:MM:SS]*	Configures the start time for RLDP schedule for the day.
end *[HH:MM:SS]*	Configures the end time for RLDP schedule for the day.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to configure the day of the week, when RLDP scheduling is to be done:

```
Device(config)# wireless wps rogue ap rldp schedule day friday start 10:10:10 end 15:15:15
```

wireless wps rogue ap timeout

To configure the expiry time for rogue APs, in seconds, use the **wireless wps rogue ap timeout** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap timeout *240-3600*

no wireless wps rogue ap timeout *240-3600*

Syntax Description

rogue ap timeout	Configures the expiry time for rogue APs, in seconds.
240-3600	Specifies the number of seconds before rogue entries are flushed.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None

Example

This example shows how to configure the expiry time for rogue APs, in seconds:

```
Device(config)# wireless wps rogue ap timeout 250
```

wireless wps rogue auto-contain

To configure the auto contain level and to configure auto containment for monitor AP mode, use the **wireless wps rogue auto-contain** command. To disable the configuration, use the **no** form of this command.

wireless wps rogue auto-contain { **level** *1 - 4* | **monitor-ap-only** }

no wireless wps rogue auto-contain { **level** *1 - 4* | **monitor-ap-only** }

Syntax Description

auto-contain	Configures auto contain for rogue devices.
level	Configures auto contain levels.
1 - 4	Specifies the auto containment levels.
monitor-ap-only	Configures auto contain for monitor AP mode.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None

Example

This example shows how to configure the auto contain level and to configure auto containment for monitor AP mode:

```
Device(config)# wireless wps rogue auto-contain level 2
Device(config)# wireless wps rogue auto-contain monitor-ap-only
```

wireless wps rogue client aaa

To configure the use of AAA or local database to detect valid MAC addresses of rogue clients, use the **wireless wps rogue client aaa** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue client aaa

no wireless wps rogue client aaa

Syntax Description

aaa	Configures the use of AAA or local database to detect valid MAC addresses of rogue clients.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to configure the use of AAA or local database to detect valid MAC addresses of rogue clients:

```
Device(config)# wireless wps rogue client aaa
```

wireless wps rogue client mse

To configure Mobility Services Engine (MSE) to detect valid MAC addresses of rogue clients, use the **wireless wps rogue client mse** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue client mse

no wireless wps rogue client mse

Syntax Description

mse	Configures the MSE to detect valid MAC addresses of rogue clients.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to configure Mobility Services Engine (MSE) to detect valid MAC addresses of rogue clients:

```
Device(config)# wireless wps rogue client mse
```

wireless wps rogue client client-threshold

To configure rogue client per a rogue AP SNMP trap threshold, use the **wireless wps rogue client client-threshold** command. To disable the configuration, use the **no** form of this command.

wireless wps rogue client client-threshold *0 - 256*

no wireless wps rogue client client-threshold *0 - 256*

Syntax Description

rogue client	Configures rogue clients.
client-threshold	Configures the rogue client per a rogue AP SNMP trap threshold.
0 - 256	Specifies the client threshold.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None

Example

This example shows how to configure rogue client per a rogue AP SNMP trap threshold:

```
Device(config)# wireless wps rogue ap timeout 250
```

wireless wps rogue client notify-min-rssi

To configure the minimum RSSI notification threshold for rogue clients, use the **wireless wps rogue client notify-min-rssi** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue client notify-min-rssi *-128 - -70*

no wireless wps rogue client notify-min-rssi *-128 - -70*

Syntax Description

rogue clients	Configures rogue clients.
notify-min-rssi	Configures the minimum RSSI notification threshold for rogue clients.
-128 - -70	Specifies the RSSI threshold in decibels.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None

Example

This example shows how to configure the minimum RSSI notification threshold for rogue clients:

```
Device(config)# wireless wps rogue client notify-min-rssi -125
```

wireless wps rogue client notify-rssi-deviation

To configure the RSSI deviation notification threshold for rogue clients, use the **wireless wps rogue client notify-rssi-deviation** command. To disable the configuration, use the **no** form of this command.

wireless wps rogue client notify-rssi-deviation *0 - 10*

no wireless wps rogue client notify-rssi-deviation *0 - 10*

Syntax Description

notify-rssi-deviation	Configures the RSSI deviation notification threshold for rogue clients.
0 - 10	Specifies the RSSI threshold in decibels.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None

Example

This example shows how to configure the RSSI deviation notification threshold for rogue clients:

```
Device(config)# wireless wps rogue client notify-rssi-deviation 6
```

wireless wps rogue rule

To configure rogue classification rule, use the **wireless wps rogue rule** command.

wireless wps rogue rule *rule-name* **priority** *priority* {**classify**{**friendly** | **malicious**} | **condition** {**client-count number** | **duration** | **encryption** | **infrastructure** | **rssi** | **ssid**} | **default** | **exit** | **match**{**all** | **any**} | **no** | **shutdown**}

Syntax Description

rule *rule-name*	Specifies a rule name.
priority *priority*	Changes the priority of a specific rule and shifts others in the list accordingly.
classify	Specifies the classification of a rule.
friendly	Classifies a rule as friendly.
malicious	Classifies a rule as malicious.
condition {**client-count number** | **duration** | **encryption** | **infrastructure** | **rssi** | **ssid**}	Specifies the conditions for a rule that the rogue access point must meet. Type of the condition to be configured. The condition types are listed below: • client-count—Requires that a minimum number of clients be associated to a rogue access point. The valid range is 1 to 10 (inclusive). • duration—Requires that a rogue access point be detected for a minimum period of time. The valid range is 0 to 3600 seconds (inclusive). • encryption—Requires that the advertised WLAN does not have encryption enabled. • infrastructure—Requires the SSID to be known to the controller • rssi—Requires that a rogue access point have a minimum RSSI value. The range is from –95 to –50 dBm (inclusive). • ssid—Requires that a rogue access point have a specific SSID.
default	Sets the command to its default settings.
exit	Exits the sub-mode.
match {**all** | **any**}	Configures matching criteria for a rule. 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.
no	Negates a command or set its defaults.
shutdown	Shuts down the system.

Command Default

None.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None.

This example shows how to create a rule that can organize and display rogue access points as Friendly:

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# classify friendly
Device(config)# end
```

wireless wps rogue security-level

To configure the wireless WPS rogue detection security levels, use the **wireless wps rogue security-level** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue security-level { **critical** | **custom** | **high** | **low** }

no wireless wps rogue security-level { **critical** | **custom** | **high** | **low** }

Syntax Description

rogue security-level	Configures the rogue detection security level.
critical	Specifies the rogue detection setup for highly sensitive deployments.
custom	Specifies the customizable security level.
high	Specifies the rogue detection setup for medium-scale deployments.
low	Specifies the basic rogue detection setup for small-scale deployments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None

Example

This example shows how to configure the wireless WPS rogue detection security levels:

```
Device(config)# wireless wps rogue security-level critical
```

wireless-default radius server

To configure multiple radius servers, use the **wireless-default radius server** command.

wireless-default radius server *IP* **key** *secret*

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines Using this utility, you can configure a maximum of ten radius servers.

Example

This example shows how to configure multiple radius servers:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless-default radius server 9.2.58.90 key cisco123
Device(config)# end
```

wlan policy

To map a policy profile to a WLAN profile, use the **wlan policy** command.

wlan *wlan-name* **policy** *policy-name*

Syntax Description

wlan-name	Name of the WLAN profile.
policy	Map a policy profile to the WLAN profile.
policy-name	Name of the policy profile.

Command Default

None

Command Modes

config-policy-tag

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Show Commands

show aaa dead-criteria radius

To verify the dead-server-detection information for a RADIUS server, use the **show aaa dead-criteria radius** command.

show aaa dead-criteria radius *ipaddr* **auth-port** *authport* **acct-port** *acctport*

Syntax Description

ipaddr	IP address.
authport	Authentication port.
acctport	Accounting port.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

The **show aaa dead-criteria radius** *ipaddr* command displays output only if default ports are used. For non-default ports, use the **show aaa dead-criteria radius** *ipaddr* **auth-port** *authport* **acct-port** *acctport* command.

Example

The following example shows how to see the dead-server-detection information for a RADIUS server with non-default authorization and accounting ports:

```
Device# show aaa dead-criteria radius 4.4.4.4 auth-port 4444 acct-port 3333

RADIUS: No server group specified. Using radius
RADIUS Server Dead Criteria:
============================
Server Details:
Address : 4.4.4.4
Auth Port : 4444
Acct Port : 3333
Server Group : radius
Dead Criteria Details:
Configured Retransmits : 3
Configured Timeout : 5
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Dead Detect Time : 10s
Computed Retransmit Tries: 10
Statistics Gathered Since Last Successful Transaction
=====================================================
Max Computed Outstanding Transactions: 0
Max Computed Dead Detect Time: 0s
```

```
Max Computed Retransmits : 0
```

The following example shows how to see the dead-server-detection information for a RADIUS server using default ports:

```
Device# show aaa dead-criteria radius 9.3.13.37

RADIUS: No server group specified. Using radius
RADIUS Server Dead Criteria:
============================
Server Details:
Address : 9.3.13.37
Auth Port : 1812
Acct Port : 1813
Server Group : radius
Dead Criteria Details:
Configured Retransmits : 3
Configured Timeout : 30
Estimated Outstanding Access Transactions: 1
Estimated Outstanding Accounting Transactions: 0
Dead Detect Time : 10s
Computed Retransmit Tries: 10
Statistics Gathered Since Last Successful Transaction
=====================================================
Max Computed Outstanding Transactions: 4
Max Computed Dead Detect Time: 48s
Max Computed Retransmits : 30
```

show access-list

To display access control lists (ACLs) configured on the device, use the **show access-lists** command in privileged EXEC mode.

show access-lists[{*namenumber* | **hardware counters** | **ipc**}]

Syntax Description

number	(Optional) ACL number. The range is 1 to 2799.
name	(Optional) Name of the ACL.
hardware counters	(Optional) Displays the access list hardware counters.
ipc	(Optional) Display Interprocess Communication (IPC) protocol access-list configuration download information

Command Default

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

Though visible in the command-line help strings, the **rate-limit** keyword is not supported

The device supports only IP standard and extended access lists. Therefore, the allowed numbers are only 1 to 199 and 1300 to 2799.

This command also displays the MAC ACLs that are configured.

This is an example of output from the **show access-lists** command:

```
Device# show access-lists

Extended IP access list 103
    10 permit ip any any dscp af11
Extended IP access list ssm-range
    10 deny ip any 232.0.0.0 0.255.255.255
    20 permit ip any any
Extended MAC access list mac1
```

This is an example of output from the **show access-lists hardware counters** command:

```
Device# show access-lists hardware counters
 L3 ACL INPUT Statistics
     All  Drop:                      frame count: 0
     All  Bridge Only:               frame count: 0
     All  Forwarding To CPU:         frame count: 294674
     All  Forwarded:                 frame count: 2577677
```

```
    All  Drop And Log:             frame count: 0
    All  Bridge Only And Log:      frame count: 0
    All  Forwarded And Log:        frame count: 0
    All  IPv6 Drop:                frame count: 0
    All  IPv6 Bridge Only:         frame count: 0
    All  IPv6 Forwarding To CPU:   frame count: 0
    All  IPv6 Forwarded:           frame count: 102
    All  IPv6 Drop And Log:        frame count: 0
    All  IPv6 Bridge Only And Log: frame count: 0
    All  IPv6 Forwarded And Log:   frame count: 0

L3 ACL OUTPUT Statistics
    All  Drop:                     frame count: 0
    All  Bridge Only:              frame count: 0
    All  Forwarding To CPU:        frame count: 0
    All  Forwarded:                frame count: 266050
    All  Drop And Log:             frame count: 0
    All  Bridge Only And Log:      frame count: 0
    All  Forwarded And Log:        frame count: 0
    All  IPv6 Drop:                frame count: 0
    All  IPv6 Bridge Only:         frame count: 0
    All  IPv6 Forwarding To CPU:   frame count: 0
    All  IPv6 Forwarded:           frame count: 0
    All  IPv6 Drop And Log:        frame count: 0
    All  IPv6 Bridge Only And Log: frame count: 0
    All  IPv6 Forwarded And Log:   frame count: 0
```

show ap auth-list

To see the access point authorization list, use the **show ap auth-list** command.

show ap auth-list [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

chassis-number	Chassis number as either 1 or 2.
active R0	Active instance in Route-processor slot 0.
standby R0	Standby instance in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the access point authorization list:

```
Device# show ap auth-list
```

show ap auto-rf

To display the auto-RF settings for a Cisco lightweight access point, use the **show ap auto-rf** command.

show ap auto-rf dot11 {**24ghz** | **5ghz** | **dual-band**} *cisco_ap*

Syntax Description

24ghz	Specifies the 802.11b AP.
5ghz	Specifies the 802.11a AP.
dual-band	Specifies dual bands.

Command Default

None

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.12.1.

Usage Guidelines

The **show ap auto-rf command** output will not display neighbor AP names.

The following example shows how to display auto-RF information for an access point:

```
Device# show ap auto-rf dot11 24ghz AP1

######################################################################

Number of Slots                                 : 3
AP Name                                         : APA023.9FD8.EA22
MAC Address                                     : 40ce.24bf.8ca0
Ethernet MAC Address                            : a023.9fd8.ea22
  Slot ID                                       : 0
  Radio Type                                    : 802.11n - 2.4 GHz
  Current TX/RX Band                            : 2.4Ghz band
  Subband Type                                  : All
  Noise Information
    Noise Profile                               : Passed
    Channel   1                                 :  -91 dBm
    Channel   2                                 :  -67 dBm
    Channel   3                                 :  -54 dBm
    Channel   4                                 :  -55 dBm
    Channel   5                                 :  -71 dBm
    Channel   6                                 :  -85 dBm
    Channel   7                                 :  -50 dBm
    Channel   8                                 :  -54 dBm
    Channel   9                                 :  -77 dBm
    Channel  10                                 :  -88 dBm
    Channel  11                                 :  -65 dBm
  Interference Information
    Interference Profile                        : Failed
    Channel   1                                 :  -47 dBm @ 21% busy
    Channel   2                                 :  -45 dBm @  2% busy
    Channel   3                                 : -128 dBm @  0% busy
    Channel   4                                 : -128 dBm @  0% busy
    Channel   5                                 :  -48 dBm @  2% busy
    Channel   6                                 :  -45 dBm @  2% busy
```

```
  Channel   7                                     :  -42 dBm @  3% busy
  Channel   8                                     : -128 dBm @  0% busy
  Channel   9                                     : -128 dBm @  0% busy
  Channel  10                                     :  -39 dBm @  3% busy
  Channel  11                                     :  -46 dBm @  3% busy
  Rogue Histogram (20)
    Channel   1                                   : 36
    Channel   2                                   :  0
    Channel   3                                   :  0
    Channel   4                                   :  1
    Channel   5                                   :  0
    Channel   6                                   : 11
    Channel   7                                   :  0
    Channel   8                                   :  1
    Channel   9                                   :  3
    Channel  10                                   :  0
    Channel  11                                   : 14
Load Information
  Load Profile                                  : Failed
  Receive Utilization                           : 0%
  Transmit Utilization                          : 0%
  Channel Utilization                           : 98%
  Attached Clients                              : 0 clients
Coverage Information
  Coverage Profile                              : Passed
  Failed Clients                                : 0 clients
Client Signal Strengths
  RSSI -100 dBm                                 : 0 clients
  RSSI  -92 dBm                                 : 0 clients
  RSSI  -84 dBm                                 : 0 clients
  RSSI  -76 dBm                                 : 0 clients
  RSSI  -68 dBm                                 : 0 clients
  RSSI  -60 dBm                                 : 0 clients
  RSSI  -52 dBm                                 : 0 clients
Client Signal to Noise Ratios
  SNR    0 dB                                   : 0 clients
  SNR    5 dB                                   : 0 clients
  SNR   10 dB                                   : 0 clients
  SNR   15 dB                                   : 0 clients
  SNR   20 dB                                   : 0 clients
  SNR   25 dB                                   : 0 clients
  SNR   30 dB                                   : 0 clients
  SNR   35 dB                                   : 0 clients
  SNR   40 dB                                   : 0 clients
  SNR   45 dB                                   : 0 clients
Nearby APs
  AP d0ec.3572.b9a0 slot 0                      :  -23 dBm on ( 11, 20 MHz) (181.22.0.22)
  AP 0c75.bdb3.9000 slot 0                      :  -28 dBm on ( 11, 20 MHz) (181.21.0.21)
  AP a4b2.3980.3740 slot 0                      :  -28 dBm on (  1, 20 MHz) (181.21.0.21)
  AP d0ec.3576.8320 slot 0                      :  -33 dBm on ( 11, 20 MHz) (50.1.1.122)
  AP a0f8.49dc.9780 slot 0                      :  -34 dBm on (  1, 20 MHz) (9.9.57.94)
  AP a0f8.49dc.8260 slot 0                      :  -34 dBm on (  6, 20 MHz) (9.9.57.94)
  AP d0ec.3573.7c80 slot 0                     :  -36 dBm on (  6, 20 MHz) (192.185.183.44)

  AP 00b0.e192.9d20 slot 0                      :  -36 dBm on ( 11, 20 MHz) (9.9.42.47)
  AP a4b2.397f.41c0 slot 0                      :  -36 dBm on (  1, 20 MHz) (185.10.0.10)
  AP 2c5a.0fd5.b8c0 slot 0                      :  -36 dBm on (  6, 20 MHz) (9.7.97.51)
  AP a488.7351.4740 slot 0                      :  -36 dBm on ( 11, 20 MHz) (9.7.97.51)
  AP 10b3.d5e9.c8e0 slot 0                      :  -36 dBm on (  1, 20 MHz) (50.1.1.122)
  AP 0c75.bdb3.ab00 slot 0                      :  -37 dBm on (  6, 20 MHz) (185.10.0.10)
  AP 68ca.e451.5120 slot 0                      :  -37 dBm on (  1, 20 MHz) (9.4.155.15)
  AP a0f8.49dc.97a0 slot 0                      :  -37 dBm on ( 11, 20 MHz) (9.9.57.94)
  AP 188b.4501.7940 slot 0                      :  -38 dBm on ( 11, 20 MHz) (9.9.57.94)
  AP 002c.c88a.f8e0 slot 0                      :  -38 dBm on ( 11, 20 MHz) (9.9.50.55)
```

```
  AP 7069.5a78.4960 slot 0                    :  -38 dBm on ( 11, 20 MHz) (9.7.97.51)
  AP 3c41.0ea7.0880 slot 0                    :  -39 dBm on ( 11, 20 MHz) (185.10.0.10)
  AP a0f8.49dc.93a0 slot 0                    :  -39 dBm on (  6, 20 MHz) (9.9.57.94)
  AP f4db.e685.7360 slot 0                    :  -39 dBm on (  6, 20 MHz) (50.1.1.122)
  AP 7070.8bb4.4120 slot 0                    :  -40 dBm on ( 11, 20 MHz) (9.9.57.94)
  AP 707d.b93e.39e0 slot 0                    :  -40 dBm on (  1, 20 MHz) (4.4.4.1)
  AP 706d.150c.6860 slot 0                    :  -40 dBm on ( 11, 20 MHz) (50.1.1.122)
Radar Information
Channel Assignment Information via DCA
  Current Channel Average Energy                :  -50 dBm
  Previous Channel Average Energy               :  -50 dBm
  Channel Change Count                          : 9
  Last Channel Change Time                      : 02/14/2021 20:54:57
  Recommended Best Channel                      : 1
RF Parameter Recommendations
  Power Level                                   : 8
  RTS/CTS Threshold                             : 2347
  Fragmentation Threshold                       : 2346
  Antenna Pattern                               : 0
Persistent Interference Devices
Class Type                Channel  DC (%%)  RSSI (dBm)  Last Update Time
------------------------  -------  ------   ---------   ----------------
All third party trademarks are the property of their respective owners.
```

show ap config

To display configuration settings for all access points that join the switch, use the **show ap config** command.

show ap config {**general** | **slots**}

Syntax Description

ethernet	Displays ethernet related information for all Cisco APs.
general	Displays common information for all Cisco APs.
slots	Displays configuration information for all slots of all Cisco APs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

This example shows how to display global syslog server settings:

```
Device# show ap config general
Cisco AP Name   : APA023.9FAE.E190
================================================

Cisco AP Identifier                              : 40ce.24f7.50e0
Country Code                                     : US
Regulatory Domain Allowed by Country             : 802.11bg:-A   802.11a:-AB
AP Country Code                                  : US  - United States
AP Regulatory Domain
  Slot 0                                         : -B
  Slot 1                                         : -B
MAC Address                                      : a023.9fae.e190
IP Address Configuration                         : DHCP
IP Address                                       : 9.12.33.244
IP Netmask                                       : 255.255.255.0
Gateway IP Address                               : 9.12.33.1
Fallback IP Address Being Used                   :
Domain                                           :
Name Server                                      :
CAPWAP Path MTU                                  : 1485
Capwap Active Window Size                        : 1
Telnet State                                     : Disabled
SSH State                                        : Disabled
Cisco AP Location                                : default location
Site Tag Name                                    : default-site-tag
RF Tag Name                                      : default-rf-tag
Policy Tag Name                                  : default-policy-tag
AP join Profile                                  : default-ap-profile
Flex Profile                                     : default-flex-profile
Primary Cisco Controller Name                    : ewlc-doc-17.1.1
Primary Cisco Controller IP Address              : 9.12.35.10
Secondary Cisco Controller Name                  : Doc-86
Secondary Cisco Controller IP Address            : 9.12.33.10
Tertiary Cisco Controller Name                   : Cisco-docvwlc-85
```

```
Tertiary Cisco Controller IP Address            : 9.12.35.16
Administrative State                            : Enabled
Operation State                                 : Registered
NAT External IP Address                         : 9.12.33.244
AP Certificate type                             : Manufacturer Installed Certificate
AP Mode                                         : Local
AP VLAN tagging state                           : Disabled
AP VLAN tag                                     : 0
.
.
.
```

show ap crash-file

To display the list of both crash and radio core dump files generated by lightweight access points, use the **show ap crash-file** command.

show ap crash-filechassis *chassis-number <1-2>***active standby**

Syntax Description

chassis	Displays the chassis details.
chassis-number	Specifies the chassis number, either 1 or 2.
active	Specifies an active instance.
standby	Specifies a standby instance.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

This example shows how to display the crash file generated by the access point:

```
Device# show ap crash-file
```

show ap dot11

To view 802.11a or 802.11b configuration information, use the **show ap dot11** command.

show ap dot11{**24ghz** | **5ghz**} {**channel** | **coverage** | **group** | **load-info** | **logging** | **media-stream** | **monitor** | **network** | **profile** | **summary** | **txpower** | }

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
channel	Displays the automatic channel assignment configuration and statistics.
coverage	Displays the configuration and statistics for coverage hole detection.
group	Displays 802.11a or 802.11b Cisco radio RF grouping.
load-info	Displays channel utilization and client count information for all Cisco APs.
logging	Displays 802.11a or 802.11b RF event and performance logging.
media-stream	Display 802.11a or 802.11b Media Resource Reservation Control configurations.
monitor	Displays the 802.11a or 802.11b default Cisco radio monitoring.
network	Displays the 802.11a or 802.11b network configuration.
profile	Displays the 802.11a or 802.11b lightweight access point performance profiles.
receiver	Displays the configuration and statistics of the 802.11a or 802.11b receiver.
summary	Displays the 802.11a or 802.11b Cisco lightweight access point name, channel, and transmit level summary.
txpower	Displays the 802.11a or 802.11b automatic transmit power assignment.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

This example shows how to display the automatic channel assignment configuration and statistics:

```
Device# show ap dot11 5ghz channel
Automatic Channel Assignment
  Channel Assignment Mode                     : AUTO
  Channel Update Interval                     : 12 Hours
  Anchor time (Hour of the day)               : 20
  Channel Update Contribution                 : SNI.
  Channel Assignment Leader                   : web (9.9.9.2)
  Last Run                                    : 13105 seconds ago
  DCA Sensitivity Level                       : MEDIUM (15 dB)
  DCA 802.11n Channel Width                   : 40 Mhz
  Channel Energy Levels
      Minimum                                 : unknown
      Average                                 : unknown
      Maximum                                 : unknown
  Channel Dwell Times
      Minimum                                 : unknown
      Average                                 : unknown
      Maximum                                 : unknown
  802.11a 5 GHz Auto-RF Channel List
  Allowed Channel List                        : 36,40,44,48,52,56,60,64,149,153,1
57,161
  Unused Channel List                         : 100,104,108,112,116,132,136,140,1
65
  802.11a 4.9 GHz Auto-RF Channel List
  Allowed Channel List                        :
  Unused Channel List                         : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20,21,22,23,24,25,26
  DCA Outdoor AP option                       : Disabled
```

This example shows how to display the statistics for coverage hole detection:

```
Device# show ap dot11 5ghz coverage
Coverage Hole Detection
  802.11a Coverage Hole Detection Mode          : Enabled
  802.11a Coverage Voice Packet Count           : 100 packet(s)
  802.11a Coverage Voice Packet Percentage      : 50 %
  802.11a Coverage Voice RSSI Threshold         : -80dBm
  802.11a Coverage Data Packet Count            : 50 packet(s)
  802.11a Coverage Data Packet Percentage       : 50 %
  802.11a Coverage Data RSSI Threshold          : -80dBm
  802.11a Global coverage exception level       : 25
  802.11a Global client minimum exception level   : 3 clients
```

This example shows how to display Cisco radio RF group settings:

```
Device# show ap dot11 5ghz group
Radio RF Grouping

  802.11a Group Mode                : STATIC
  802.11a Group Update Interval     : 600 seconds
  802.11a Group Leader              : web (10.10.10.1)
  802.11a Group Member              : web(10.10.10.1)
                                      nb1(172.13.21.45) (*Unreachable)
  802.11a Last Run                  : 438 seconds ago


  Mobility Agents RF membership information
  ------------------------------------------------------------
  No of 802.11a MA RF-members : 0
```

This example shows how to display 802.11a RF event and performance logging:

```
Device# show ap dot11 5ghz logging
RF Event and Performance Logging

  Channel Update Logging             : Off
  Coverage Profile Logging           : Off
  Foreign Profile Logging            : Off
  Load Profile Logging               : Off
  Noise Profile Logging              : Off
  Performance Profile Logging        : Off
  TxPower Update Logging             : Off
```

This example shows how to display the 802.11a media stream configuration:

```
Device# show ap dot11 5ghz media-stream
Multicast-direct                : Disabled
Best Effort                     : Disabled
Video Re-Direct                 : Disabled
Max Allowed Streams Per Radio     : Auto
Max Allowed Streams Per Client    : Auto
Max Video Bandwidth              : 0
Max Voice Bandwidth              : 75
Max Media Bandwidth              : 85
Min PHY Rate (Kbps)              : 6000
Max Retry Percentage             : 80
```

This example shows how to display the radio monitoring for the 802.11b network:

```
Device# show ap dot11 5ghz monitor
Default 802.11a AP monitoring

  802.11a Monitor Mode                         : Enabled
  802.11a Monitor Mode for Mesh AP Backhaul    : disabled
  802.11a Monitor Channels                     : Country channels
  802.11a RRM Neighbor Discover Type           : Transparent
  802.11a AP Coverage Interval                 : 180 seconds
  802.11a AP Load Interval                     : 60 seconds
  802.11a AP Noise Interval                    : 180 seconds
  802.11a AP Signal Strength Interval          : 60 seconds
```

This example shows how to display the global configuration and statistics of an 802.11a profile:

```
Device# show ap dot11 5ghz profile
Default 802.11a AP performance profiles
802.11a Global Interference threshold.............. 10%
802.11a Global noise threshold..................... -70 dBm
802.11a Global RF utilization threshold............ 80%
802.11a Global throughput threshold................ 1000000 bps
802.11a Global clients threshold................... 12 clients
802.11a Global coverage threshold.................. 12 dB
802.11a Global coverage exception level............ 80%
802.11a Global client minimum exception lev........ 3 clients
```

This example shows how to display the network configuration of an 802.11a profile:

```
Device# 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 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
```

This example shows how to display the global configuration and statistics of an 802.11a profile:

```
Device# show ap dot11 5ghz receiver
Default 802.11a AP performance profiles
802.11a Global Interference threshold.............. 10%
802.11a Global noise threshold..................... -70 dBm
802.11a Global RF utilization threshold............ 80%
802.11a Global throughput threshold................ 1000000 bps
802.11a Global clients threshold................... 12 clients
802.11a Global coverage threshold.................. 12 dB
802.11a Global coverage exception level............ 80%
802.11a Global client minimum exception lev........ 3 clients
```

This example shows how to display the global configuration and statistics of an 802.11a profile:

```
Device# show ap dot11 5ghz service-policy
```

This example shows how to display a summary of the 802.11b access point settings:

```
Device# show ap dot11 5ghz summary
AP Name MAC Address       Admin State Operation State Channel TxPower
------- ----------------- ----------- --------------- ------- -------
CJ-1240 00:21:1b:ea:36:60 ENABLED     UP              161     1( )
CJ-1130 00:1f:ca:cf:b6:60 ENABLED     UP              56*     1(*)
```

This example shows how to display the configuration and statistics of the 802.11a transmit power cost:

```
Device# show ap dot11 5ghz txpower
Automatic Transmit Power Assignment

Transmit Power Assignment Mode          : AUTO
Transmit Power Update Interval          : 600 seconds
Transmit Power Threshold                : -70 dBm
Transmit Power Neighbor Count           : 3 APs
Min Transmit Power                      : -10 dBm
```

```
Max Transmit Power                        : 30 dBm
Transmit Power Update Contribution        : SNI.
Transmit Power Assignment Leader          : web (10.10.10.1)
Last Run                                  : 437 seconds ago
```

This example shows how to display the configuration and statistics of the 802.11a transmit power cost:

```
Device# show ap dot11 5ghz ccx global
 802.11a Client Beacon Measurements:
     disabled
```

show ap dot11

To display 802.11 band parameters, use the **show ap dot11** command.

show ap dot11 {**24ghz** | **5ghz**} {**media-stream rrc**}

Syntax Description

media-stream rrc	Displays Media Stream configurations.

Command Default

None

Command Modes

User EXEC command mode or Privileged EXEC command mode

Usage Guidelines

None.

The following is a sample output of the **show ap dot11 24ghz media-stream rrc** command.

```
Device#show ap dot11 24ghz media-stream rrc

Multicast-direct                : Disabled
Best Effort                     : Disabled
Video Re-Direct                 : Disabled
Max Allowed Streams Per Radio      : Auto
Max Allowed Streams Per Client     : Auto
Max Video Bandwidth              : 0
Max Voice Bandwidth              : 75
Max Media Bandwidth              : 85
Min PHY Rate (Kbps)              : 6000
Max Retry Percentage             : 80
```

show ap dot11 24ghz

To display the 2.4 GHz RRM parameters, use the **show ap dot11 24ghz** command.

show ap dot11 24ghz {**channel** | **coverage** | **group** | **logging** | **monitor** | **profile** | **summary** | **txpower**}

Syntax Description

ccx	Displays the 802.11b CCX information for all Cisco APs.
channel	Displays the configuration and statistics of the 802.11b channel assignment.
coverage	Displays the configuration and statistics of the 802.11b coverage.
group	Displays the configuration and statistics of the 802.11b grouping.
l2roam	Displays 802.11b l2roam information.
logging	Displays the configuration and statistics of the 802.11b event logging.
monitor	Displays the configuration and statistics of the 802.11b monitoring.
profile	Displays 802.11b profiling information for all Cisco APs.
receiver	Displays the configuration and statistics of the 802.11b receiver.
summary	Displays the configuration and statistics of the 802.11b Cisco APs.
txpower	Displays the configuration and statistics of the 802.11b transmit power control.

Command Default

None.

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Usage Guidelines

None.

This example shows how to display configuration and statistics of the 802.11b coverage.

```
Device#show ap dot11 24ghz coverage

Coverage Hole Detection
  802.11b Coverage Hole Detection Mode            : Enabled
  802.11b Coverage Voice Packet Count             : 100 packet(s)
  802.11b Coverage Voice Packet Percentage        : 50%
  802.11b Coverage Voice RSSI Threshold           : -80 dBm
  802.11b Coverage Data Packet Count              : 50 packet(s)
  802.11b Coverage Data Packet Percentage         : 50%
  802.11b Coverage Data RSSI Threshold            : -80 dBm
  802.11b Global coverage exception level         : 25 %
  802.11b Global client minimum exception level   : 3 clients
```

show ap dot11 24ghz SI config

To see the spectrum intelligence (SI) configuration details for the 2.4-GHz band, use the **show ap dot11 24ghz SI config** command.

show ap dot11 24ghz SI config [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

chassis-number	Chassis number as either 1 or 2.
active R0	Active instance of the configuration in Route-processor slot 0.
standby R0	Standby instance of the configuration in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the SI configuration details for the 2.4-GHz band:

```
Device# show ap dot11 24ghz SI config chassis 1 R0
```

show ap dot11 24ghz SI device type

To see the spectrum intelligence (SI) interferers of different types for the 2.4-GHz band, use the **show ap dot11 24ghz SI device type** command.

show ap dot11 24ghz SI device type {**cont_tx** | **mw_oven** | **si_fhss**} [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

cont_tx	SI interferers of type Continuous transmitter for the 2.4-GHz band.
mw_oven	SI interferers of type microwave oven for the 2.4-GHz band.
si_fhss	SI interferers of type Frequency Hopping Spread Spectrum for the 2.4-GHz band.
chassis-number	Enter the chassis number as either 1 or 2.
active R0	Active instance of the configuration in Route-processor slot 0.
standby R0	Standby instance of the configuration in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the details of SI interferers of type microwave oven in the 2.4-GHz band:

```
Device# show ap dot11 24ghz SI device type mw_oven chassis 1 R0
```

show ap dot11 5ghz

To display the 5GHz RRM parameters, use the **show ap dot11 5ghz** command.

show ap dot11 5ghz {**channel** | **coverage** | **group** | **logging** | **monitor** | **profile** | **summary** | **txpower**}

Syntax Description

ccx	Displays the 802.11a CCX information for all Cisco APs.
channel	Displays the configuration and statistics of the 802.11a channel assignment.
coverage	Displays the configuration and statistics of the 802.11a coverage.
group	Displays the configuration and statistics of the 802.11a grouping.
l2roam	Displays 802.11a l2roam information.
logging	Displays the configuration and statistics of the 802.11a event logging.
monitor	Displays the configuration and statistics of the 802.11a monitoring.
profile	Displays 802.11a profiling information for all Cisco APs.
receiver	Displays the configuration and statistics of the 802.11a receiver.
summary	Displays the configuration and statistics of the 802.11a Cisco APs.
txpower	Displays the configuration and statistics of the 802.11a transmit power control.

Command Default

None.

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Usage Guidelines

None.

This example shows configuration and statistics of 802.11a channel assignment.

```
Device#show ap dot11 5ghz channel

Automatic Channel Assignment
  Channel Assignment Mode                   : AUTO
  Channel Update Interval                   : 12 Hours
  Anchor time (Hour of the day)             : 20
  Channel Update Contribution               : SNI..
  Channel Assignment Leader                 : web (9.9.9.2)
  Last Run                                  : 16534 seconds ago
  DCA Sensitivity Level                     : MEDIUM (15 dB)
  DCA 802.11n Channel Width                 : 40 Mhz
  Channel Energy Levels
      Minimum                               : unknown
```

```
    Average                                 : unknown
    Maximum                                 : unknown
Channel Dwell Times
    Minimum                                 : unknown
    Average                                 : unknown
    Maximum                                 : unknown
802.11a 5 GHz Auto-RF Channel List
Allowed Channel List                        : 36,40,44,48,52,56,60,64,149,153,1

              57,161
Unused Channel List                         : 100,104,108,112,116,132,136,140,1

              65
802.11a 4.9 GHz Auto-RF Channel List
Allowed Channel List                        :
Unused Channel List                         : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,

              15,16,17,18,19,20,21,22,23,24,25,26
DCA Outdoor AP option                       : Disabled
```

show ap dot11 24ghz cleanair air-quality

To display the air-quality summary information and air-quality worst information for the 802.11 networks, use the **show ap dot11 cleanair** command.

show ap dot11 {**24ghz** | **5ghz** | **dual-band**} **cleanair** {**air-quality** | **config** | **device** | **summary**}

Syntax Description

24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.
dual-band	Displays 802.11 dual-band radios.
cleanair	Displays cleanair configurations.
air-quality	Displays the Cleanair Air-Quality (AQ) data for 2.4GHz band.
device	Displays the CleanAir Interferers of device for 2.4GHz band.
config	Displays CleanAir Configuration for 2.4GHz band.
summary	Displays cleanair configurations for all 802.11a Cisco APs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

This example shows how to display the worst air-quality information for the 5 GHz band:

```
Device# show ap dot11 5ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
------------ ------- ------ ------ ----------- -----
CISCO_AP3500 36      95     70     0           40
```

This example shows how to display the worst air-quality information for the 2.4 GHz band:

```
Device# show ap dot11 24ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
------------ ------- ------ ------ ----------- -----
CISCO_AP3500 1       83     57     3           5
```

show ap dot11 24ghz cleanair air-quality

To display the air-quality summary information and air-quality worst information for the 802.11 networks, use the **show ap dot11 cleanair air-quality** command.

show ap dot11 {**24ghz** | **5ghz**} **cleanair air-quality** {**summary** | **worst**}

Syntax Description

24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.
summary	Displays a summary of 802.11 radio band air-quality information.
worst	Displays the worst air-quality information for 802.11 networks.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

This example shows how to display the worst air-quality information for the 5 GHz band:

```
Device# show ap dot11 5ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
------------ ------- ------ ------ ----------- -----
CISCO_AP3500 36      95     70     0           40
```

This example shows how to display the worst air-quality information for the 2.4 GHz band:

```
Device# show ap dot11 24ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
------------ ------- ------ ------ ----------- -----
CISCO_AP3500 1       83     57     3           5
```

show ap dot11 cleanair config

To display the CleanAir configuration for the 802.11 networks, use the **show ap dot11 cleanair config** command.

show ap dot11 {**24ghz** | **5ghz**} **cleanair config**

Syntax Description

24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to display the CleanAir configuration for the 2.4 GHz band:

```
Device# show ap dot11 24ghz cleanair config
Clean Air Solution..............................: Disabled
Air Quality Settings:
    Air Quality Reporting.......................: Disabled
    Air Quality Reporting Period (min)..........: 15
    Air Quality Alarms..........................: Enabled
    Air Quality Alarm Threshold.................: 10
Interference Device Settings:
    Interference Device Reporting...............: Enabled
        Bluetooth Link..........................: Enabled
        Microwave Oven..........................: Enabled
        802.11 FH...............................: Enabled
        Bluetooth Discovery.....................: Enabled
        TDD Transmitter.........................: Enabled
        Jammer..................................: Enabled
        Continuous Transmitter..................: Enabled
        DECT-like Phone.........................: Enabled
        Video Camera............................: Enabled
        802.15.4................................: Enabled
        WiFi Inverted...........................: Enabled
        WiFi Invalid Channel....................: Enabled
        SuperAG.................................: Enabled
        Canopy..................................: Enabled
        Microsoft Device........................: Enabled
        WiMax Mobile............................: Enabled
        WiMax Fixed.............................: Enabled
    Interference Device Types Triggering Alarms:
        Bluetooth Link..........................: Disabled
        Microwave Oven..........................: Disabled
        802.11 FH...............................: Disabled
        Bluetooth Discovery.....................: Disabled
        TDD Transmitter.........................: Disabled
        Jammer..................................: Disabled
        Continuous Transmitter..................: Disabled
        DECT-like Phone.........................: Disabled
```

```
        Video Camera.............................. : Disabled
        802.15.4.................................. : Disabled
        WiFi Inverted............................. : Enabled
        WiFi Invalid Channel...................... : Enabled
        SuperAG................................... : Disabled
        Canopy.................................... : Disabled
        Microsoft Device.......................... : Disabled
        WiMax Mobile.............................. : Disabled
        WiMax Fixed............................... : Disabled
    Interference Device Alarms.................... : Enabled
Additional Clean Air Settings:
    CleanAir Event-driven RRM State............... : Disabled
    CleanAir Driven RRM Sensitivity............... : LOW
    CleanAir Persistent Devices state............. : Disabled
```

show ap dot11 cleanair summary

To view CleanAir configurations for all 802.11a Cisco APs, use the **show ap dot11 cleanair summary** command.

show ap dot11{**24ghz** | **5ghz**} **cleanair summary**

Syntax Description

24ghz	Specifies the 2.4-GHz band
5ghz	Specifies the 5-GHz band
cleanair summary	Summary of CleanAir configurations for all 802.11a Cisco APs

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

show ap dot11 dual-band summary

To view a brief summary of access points with dual-band radios, use the **show ap dot11 dual-band summary** command.

show ap dot11 dual-band summary

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC

Command History

Example

The following example shows how to view brief summary of tag names:

```
Device# show ap dot11 dual-band summary
```

show ap environment

To see the AP environment information of all APs, use the **show ap environment** command.

show ap environment [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

chassis-number	Enter the chassis number as either 1 or 2.
active R0	Active instance of the AP filters in Route-processor slot 0.
standby R0	Standby instance of the AP filters in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the AP environment information:

```
Device# show ap environment
```

show ap filters active

To see the details of active AP filters, use the **show ap filters active** command.

show ap filters active [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

chassis-number	Chassis number as either 1 or 2.
active R0	Active instance of the active AP filters in Route-processor slot 0.
standby R0	Standby instance of the active AP filters in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the details of the active AP filters for the active instance:

```
Device# show ap filters active chassis active R0
```

show ap filters all

To see the details of all AP filters, use the **show ap filters all** command.

show ap filters all [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

chassis-number	Enter the chassis number as either 1 or 2.
active R0	Active instance of the AP filters in Route-processor slot 0.
standby R0	Standby instance of the AP filters in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the details of all the AP filters for the active instance:

```
Device# show ap filters all chassis active R0
```

show ap fra

To see the flexible radio assignment (FRA) configurations in APs, use the **show ap fra** command.

show ap fra [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

chassis-number	Chassis number as either 1 or 2.
active R0	Active instance in Route-processor slot 0.
standby R0	Standby instance in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the FRA configurations in APs:

```
Device# show ap fra
```

show ap gps location

To see the GPS location of all APs, use the **show ap gps location** command.

show ap gps location [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

chassis-number	Enter the chassis number as either 1 or 2.
active R0	Active instance of the AP filters in Route-processor slot 0.
standby R0	Standby instance of the AP filters in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the GPS location of all APs:

```
Device# show ap gps location
```

show history channel interface dot11Radio all

To check channel change or trigger reason and history, use the **show history channel interface dot11Radio all** command.

show history channel interface dot11Radio all

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

Examples

This example shows how to check channel change or trigger reason and history:

```
Device# show history channel interface dot11Radio all

               Timestamp Slot Client count Channel Trigger
Fri May 31 12:57:04 2019    0            0      11 RRM-DCA
Fri May 31 13:10:02 2019    0            0       1 RRM-DCA
Fri May 31 12:57:04 2019    1            0      60  Manual
Fri May 31 13:00:16 2019    1            0     149     DFS
```

show ap link-encryption

To display the link encryption status, use the **show ap link-encryption** command.

show ap link-encryption[{**chassis** | {*chassis-number* | **active** | **standby**} | **R0**}]

Syntax Description

chassis-number	Chassis number as either 1 or 2.
active R0	Active instance in Route-processor slot 0.
standby R0	Standby instance in Route-processor slot 0.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

This example show how to display the link-encryption status:

```
Device# show Cisco IOS XE Gibraltar 16.12.2s link-encryption
```

show ap master list

To see the AP master list, use the **show ap master list** command.

show ap master list[{**chassis** | {*chassis-number* | **active** | **standby**} | **R0**}]

Syntax Description

chassis-number	Chassis number as either 1 or 2.
active R0	Active instance in Route-processor slot 0.
standby R0	Standby instance in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the AP master list:

```
Device# show ap master list
```

show ap multicast mom (multicast over multicast)

To verify the multicast mode on the controller, use the **show ap multicast mom** command.

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Previleged EXEC

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2	This command was introduced.

This example shows how to verify the multicast mode:

```
Device# show ap multicast mom

AP Name                      MOM-IP     TYPE MOM- STATUS
-------------------------------------------------------
SS-E-1                       IPv4            Up
SS-E-2                       IPv4            Up
9130E-r3-sw2-g1012           IPv4            Up
9115i-r3-sw2-te1-0-38        IPv4            Up
AP9120-r3-sw3-Gi1-0-46       IPv4            Up
ap3800i-r2-sw1-te2-0-2       IPv4            Up
```

show ap name auto-rf

To display the auto-RF settings for a Cisco lightweight access point, use the **show ap name auto-rf** command.

show ap name *ap-name* **auto-rf dot11** {**24ghz** | **5ghz** | **dual-band**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.
dual-band	Displays dual band.

Command Default

None

Command Modes

Privileged EXEC.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

This example shows how to display auto-RF information for an access point:

```
Device# show ap name AP01 auto-rf dot11 24ghz

Number of Slots                                 : 2
AP Name                                         : TSIM_AP-1
MAC Address                                     : 0000.2000.02f0
Slot ID                                         : 0
Radio Type                                      : 802.11b/g
Subband Type                                    : All

Noise Information
  Noise Profile                                 : Failed
  Channel   1                                    :   24 dBm
  Channel   2                                    :   48 dBm
  Channel   3                                    :   72 dBm
  Channel   4                                    :   96 dBm
  Channel   5                                    :  120 dBm
  Channel   6                                    : -112 dBm
  Channel   7                                    :  -88 dBm
  Channel   8                                    :  -64 dBm
  Channel   9                                    :  -40 dBm
  Channel  10                                    :  -16 dBm
  Channel  11                                    :    8 dBm

Interference Information
  Interference Profile                          : Passed
  Channel   1                                    : -128 dBm @  0% busy
  Channel   2                                    :  -71 dBm @  1% busy
  Channel   3                                    :  -72 dBm @  1% busy
  Channel   4                                    :  -73 dBm @  2% busy
  Channel   5                                    :  -74 dBm @  3% busy
  Channel   6                                    :  -75 dBm @  4% busy
  Channel   7                                    :  -76 dBm @  5% busy
```

```
  Channel   8                                     :  -77 dBm @  5% busy
  Channel   9                                     :  -78 dBm @  6% busy
  Channel  10                                     :  -79 dBm @  7% busy
  Channel  11                                     :  -80 dBm @  8% busy

Rogue Histogram (20/40_ABOVE/40_BELOW)
    Channel  36                                   : 27/ 4/ 0
    Channel  40                                   : 13/ 0/ 0
    Channel  44                                   :  5/ 0/ 0
    Channel  48                                   :  6/ 0/ 1
    Channel  52                                   :  4/ 0/ 0
    Channel  56                                   :  5/ 0/ 0
    Channel  60                                   :  1/ 3/ 0
    Channel  64                                   :  3/ 0/ 0
    Channel 100                                   :  0/ 0/ 0
    Channel 104                                   :  0/ 0/ 0
    Channel 108                                   :  0/ 1/ 0

Load Information
  Load Profile                                    : Passed
  Receive Utilization                             : 10%
  Transmit Utilization                            : 20%
  Channel Utilization                             : 50%
  Attached Clients                                : 0 clients

Coverage Information
  Coverage Profile                                : Passed
  Failed Clients                                  : 0 clients

Client Signal Strengths
  RSSI -100 dBm                                   : 0 clients
  RSSI  -92 dBm                                   : 0 clients
  RSSI  -84 dBm                                   : 0 clients
  RSSI  -76 dBm                                   : 0 clients
  RSSI  -68 dBm                                   : 0 clients
  RSSI  -60 dBm                                   : 0 clients
  RSSI  -52 dBm                                   : 0 clients

Client Signal to Noise Ratios
  SNR    0 dB                                     : 0 clients
  SNR    5 dB                                     : 0 clients
  SNR   10 dB                                     : 0 clients
  SNR   15 dB                                     : 0 clients
  SNR   20 dB                                     : 0 clients
  SNR   25 dB                                     : 0 clients
  SNR   30 dB                                     : 0 clients
  SNR   35 dB                                     : 0 clients
  SNR   40 dB                                     : 0 clients
  SNR   45 dB                                     : 0 clients

Nearby APs
  AP 0000.2000.0300 slot 0                        : -68 dBm on  11 (10.10.10.1)
  AP 0000.2000.0400 slot 0                        : -68 dBm on  11 (10.10.10.1)
  AP 0000.2000.0600 slot 0                        : -68 dBm on  11 (10.10.10.1)

Radar Information

Channel Assignment Information
  Current Channel Average Energy                  : 0 dBm
  Previous Channel Average Energy                 : 0 dBm
  Channel Change Count                            : 0
  Last Channel Change Time                        : Wed Oct 17 08:13:36 2012
  Recommended Best Channel                        : 11
```

```
RF Parameter Recommendations
  Power Level                                 : 1
  RTS/CTS Threshold                           : 2347
  Fragmentation Threshold                     : 2346
  Antenna Pattern                             : 0

Persistent Interference Devices
```

show ap name ble detail

To display BLE management details, use the **show ap name ble detail** command.

show ap name *ap-name* **ble detail**

Syntax Description

ap-name	Specifies the name of the AP.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to display the BLE management details:

```
Device(config)# show ap name ap-name ble detail
```

show ap name cablemodem

To see cable modem information of an AP, use the **show ap name** *ap-name* **cablemodem** command.

show ap name *ap-name* **cablemodem** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

ap-name	Name of the AP.
chassis-number	Enter the chassis number as either 1 or 2.
active R0	Active instance of the AP filters in Route-processor slot 0.
standby R0	Standby instance of the AP filters in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see cable modem information of an AP:

```
Device# show ap name my-ap cablemodem
```

show ap name config

To display common information and Ethernet VLAN tagging information for a specific Cisco lightweight access point, use the **show ap name config** command.

show ap name *ap-name* **config** {**ethernet** | **general**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
ethernet	Displays Ethernet tagging configuration information for an access point.
general	Displays common information for an access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to display Ethernet tagging information for an access point:

```
Device# show ap name AP01 config ethernet

VLAN Tagging Information for AP01
```

This example shows how to display common information for an access point:

```
Device# show ap name AP01 config general

Cisco AP Name                                  : AP01
Cisco AP Identifier                            : 5
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                                    : 0000.2000.02f0
IP Address Configuration                       : Static IP assigned
IP Address                                     : 10.10.10.12
IP Netmask                                     : 255.255.0.0
Gateway IP Address                             : 10.10.10.1
Fallback IP Address Being Used                 : 10.10.10.12
Domain                                         : Cisco
Name Server                                    : 0.0.0.0
CAPWAP Path MTU                                : 1485
Telnet State                                   : Enabled
SSH State                                      : Disabled
Cisco AP Location                              : sanjose
Cisco AP Group Name                            : default-group
Primary Cisco Controller Name                  : CAPWAP Controller
Primary Cisco Controller IP Address            : 10.10.10.1
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                                        : 1140AG
AP Image                                        : C1140-K9W8-M
IOS Version                                     :
Reset Button                                    :
AP Serial Number                                : SIM1140K001
AP Certificate Type                             : Manufacture Installed
Management Frame Protection Validation          : Disabled
AP User Mode                                    : Customized
AP User Name                                    : cisco
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                                      : 15 days 16 hours 19 minutes 57
 seconds
AP CAPWAP Up Time                               : 4 minutes 56 seconds
Join Date and Time                              : 10/18/2012 04:48:56
Join Taken Time                                 : 15 days 16 hours 15 minutes 0
seconds
Join Priority                                   : 1
Ethernet Port Duplex                            : Auto
Ethernet Port Speed                             : Auto
AP Link Latency                                 : Disabled
Rogue Detection                                 : Disabled
AP TCP MSS Adjust                               : Disabled
AP TCP MSS Size                                 : 6146
```

show ap name config ethernet

To see Ethernet related configuration information of an AP, use the **show ap name** *ap-name* **config ethernet** command.

show ap name *ap-name* **config ethernet** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

ap-name	Name of the AP.
chassis-number	Enter the chassis number as either 1 or 2.
active R0	Active instance of the AP filters in Route-processor slot 0.
standby R0	Standby instance of the AP filters in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see Ethernet related configuration information of an AP:

```
Device# show ap name my-ap config ethernet
```

show ap name dot11

To display 802.11a or 802.11b configuration information that corresponds to specific Cisco lightweight access points, use the **show ap name dot11** command.

show ap name *ap-name* **dot11** {**24ghz** | **5ghz**} {**SI** | **airtime-fairness** | **call-control** | **cleanair radio-reset** | **voice**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.
SI	Displays the SI configurations.
airtime-fairness	Displays the stats of 24Ghz or 5Ghz airtime-fairness.
call-control	Displays the call control information.
radio-reset	Displays radio-reset.
slot	Displays slot information.
voice	Displays voice information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

This example shows how to display the cleanair air-quality that is associated with the access point:

```
Device# show ap name test-ap dot11 24ghz cleanair air-quality chassis active r0
```

show ap name environment

To see the AP environment information of an AP, use the **show ap name** *ap-name* **environment** command.

show ap name *ap-name* **environment** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

ap-name	Name of the AP.
chassis-number	Enter the chassis number as either 1 or 2.
active R0	Active instance of the AP filters in Route-processor slot 0.
standby R0	Standby instance of the AP filters in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the AP environment information of an AP:

```
Device# show ap name my-ap environment
```

show ap name gps location

To see the GPS location of the AP, use the **show ap name gps location** command.

show ap name *ap-name* **gps location** [{*chassis-number* | **active** | **standby**}**R0**

Syntax Description

ap-name	Name of the Access Point
gps	See the GPS information of a Cisco AP
location	Shows the Mesh linktest data
chassis-number	Enter the chassis number as either 1 or 2.
active R0	Active instance of the active AP filters in Route-processor slot 0.
standby R0	Standby instance of the configuration in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the GPS location of an AP:

```
Device# show ap name mesh-profile-name gps location
```

show ap name mesh neighbor detail

To see detailed information about a neighbor of a mesh AP, use the **show ap name** *ap-name* **mesh neighbor detail** command.

show ap name *ap-name* **mesh neighbor detail** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

ap-name	Name of the AP.
chassis-number	Enter the chassis number as either 1 or 2.
active R0	Active instance of the AP filters in Route-processor slot 0.
standby R0	Standby instance of the AP filters in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see detailed information about a neighbor of a mesh AP:

```
Device# show ap name mymeshap mesh neighbhor detail
```

show ap name wlan

To display the Basic Service Set Identifier (BSSID) value for each WLAN defined on an access point and to display WLAN statistics, use the **show ap name wlan** command.

show ap name *ap-name* **wlan** {**dot11** {**24ghz** | **5ghz**} | **statistic**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
dot11	Displays 802.11 parameters.
24ghz	Displays 802.11b network settings.
5ghz	Displays 802.11a network settings.
statistic	Displays WLAN statistics.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to display BSSID information of an access point in an 802.11b network:

```
Device# show ap name AP01 wlan dot11 24ghz

Site Name                                       : default-group
Site Description                                :

WLAN ID  Interface  BSSID
------------------------------------
1        default    00:00:20:00:02:00
12       default    00:00:20:00:02:0b
```

This example shows how to display WLAN statistics for an access point:

```
Device# show ap name AP01 wlan statistic

WLAN ID  : 1
WLAN Profile Name  : maria-open

   EAP Id Request Msg Timeouts           : 0
   EAP Id Request Msg Timeouts Failures  : 0
   EAP Request Msg Timeouts              : 0
   EAP Request Msg Timeouts Failures     : 0
   EAP Key Msg Timeouts                  : 0
   EAP Key Msg Timeouts Failures         : 0


WLAN ID  : 12
WLAN Profile Name  : 24
```

```
EAP Id Request Msg Timeouts           : 0
EAP Id Request Msg Timeouts Failures  : 0
EAP Request Msg Timeouts              : 0
EAP Request Msg Timeouts Failures     : 0
EAP Key Msg Timeouts                  : 0
EAP Key Msg Timeouts Failures         : 0
```

show ap profile

To see overall status of Hyperlocation for an AP profile, use the **show ap profile** command.

show ap profile *profile-name* {**detailed** | **hyperlocation** {**ble-beacon** | **detail** | **summary**}} [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

profile-name	AP profile name.
detailed	Shows the detailed parameters of the AP join profile.
hyperlocation	Shows Hyperlocation information for the AP profile.
ble-beacon	Show the list of configured BLE beacons for the AP profile.
detail	Shows detailed status of Hyperlocation for the AP profile.
summary	Shows overall status of Hyperlocation for the AP profile
chassis-number	Chassis number as either 1 or 2.
active R0	Active instance in Route-processor slot 0.
standby R0	Standby instance in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the overall status of Hyperlocation for an AP profile:

```
Device# show ap profile my-ap-profile detailed
```

show ap rf-profile name

To display the selected ap RF-Profile details, use the **show ap rf-profile name** command.

show ap rf-profile name *profile-name* **detail**

Syntax Description

profile-name	Name of the RF-Profile.
detail	Show detail of selected RF Profile.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

None

This example shows how to display the details of the selected RF-Profile.

```
Device#show ap rf-profile name doctest detail
Description :
AP Group Names :
RF Profile Name : doctest
Band : 2.4 GHz
802.11n client only : Disabled
Transmit Power Threshold v1: -70 dBm
Min Transmit Power: -10 dBm
Max Transmit Power: 30 dBm
Operational Rates
  802.11b 1M Rate : Mandatory
  802.11b 2M Rate : Mandatory
  802.11b 5.5M Rate : Mandatory
  802.11b 11M Rate : Mandatory
  802.11b 6M Rate : Mandatory
  802.11b 9M Rate : Supported
  802.11b 12M Rate : Supported
  802.11b 18M Rate : Supported
  802.11b 24M Rate : Supported
  802.11b 36M Rate : Supported
  802.11b 48M Rate : Supported
  802.11b 54M Rate : Supported
Max Clients : 200
Wlan name                       Max Clients
----------------------------------------------

Trap Threshold
  Clients:  12 clients
  Interference:  10%
  Noise:  -70 dBm
  Utilization:  80%
Multicast Data Rate: auto
Rx SOP Threshold : auto
Band Select
```

```
  Probe Response:  Disabled
  Cycle Count:  2 cycles
  Cycle Threshold:  200 milliseconds
  Expire Suppression:  20 seconds
  Expire Dual Band:  60 seconds
  Client RSSI:  -80 dBm
  Client Mid RSSI:  -80 dBm
Load Balancing
  Window:  5 clients
  Denial:  3 count
Coverage Data
  Data: -80 dBm
  Voice: -80 dBm
 Minimum Client Level: 3 clients
  Exception Level: 25%
DCA Channel List  : 1,5,9,13
DCA Foreign AP Contribution : Enabled
802.11n MCS Rates
  MCS 0 : Enabled
  MCS 1 : Enabled
  MCS 2 : Enabled
  MCS 3 : Enabled
  MCS 4 : Enabled
  MCS 5 : Enabled
  MCS 6 : Enabled
  MCS 7 : Enabled
  MCS 8 : Enabled
  MCS 9 : Enabled
  MCS 10 : Enabled
  MCS 11 : Enabled
  MCS 12 : Enabled
  MCS 13 : Enabled
  MCS 14 : Enabled
  MCS 15 : Enabled
  MCS 16 : Enabled
  MCS 17 : Enabled
  MCS 18 : Enabled
  MCS 19 : Enabled
  MCS 20 : Enabled
  MCS 21 : Enabled
  MCS 22 : Enabled
  MCS 23 : Enabled
  MCS 24 : Enabled
  MCS 25 : Enabled
  MCS 26 : Enabled
  MCS 27 : Enabled
  MCS 28 : Enabled
  MCS 29 : Enabled
  MCS 30 : Enabled
  MCS 31 : Enabled
State : Down
```

show ap rf-profile summary

To display the ap RF-Profile summary, use the **show ap rf-profile summary** command.

show ap rf-profile summary

Syntax Description

summary	Show summary of RF Profiles

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

None

This example shows how to display the ap RF-Profile summary .

```
Device#show ap rf-profile summary
Number of RF Profiles : 1

RF Profile Name                  Band      Description           Applied   State
------------------------------------------------------------------------------
doctest                          2.4 GHz                         No        Down
```

show ap summary

To display the status summary of all Cisco lightweight access points attached to the switch, use the **show ap summary** command.

show ap summary

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

Use this command to display a list that contains each lightweight access point name, number of slots, manufacturer, MAC address, location, and the switch port number.

This example shows how to display a summary of all connected access points:

```
Controller# show ap summary

Number of APs: 1

Global AP User Name: Cisco
Global AP Dot1x User Name: Not configured

AP Name                          AP Model  Ethernet MAC    Radio MAC       State
-----------------------------------------------------------------------------------
3602a                            3502I     003a.99eb.3fa8  d0c2.8267.8b00  Registered
```

show ap tag sources

To see AP tag sources with priorities, use the **show ap tag sources** command.

show ap tag sources [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

chassis-number	Chassis number as either 1 or 2.
active R0	Active instance of the AP filters in Route-processor slot 0.
standby R0	Standby instance of the AP filters in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the AP tag sources with priorities for the active instance:

```
Device# show ap tag sources chassis active R0
```

show ap tag summary

To view brief summary of tag names, use the **show ap tag summary** command.

show ap tag summary

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to view brief summary of tag names:

```
Device# show ap tag summary
```

show ap upgrade

To see AP upgrade information, use the **show ap upgrade** command.

show ap upgrade [{**name** *ap-upgrade-report-name* | **summary** | **chassis** {*chassis-number* | **active** | **standby**}}]

Syntax Description

name *ap-upgrade-report-name*	Enter the name of the AP upgrade report.
summary	Shows a summary of AP upgrade information.
chassis-number	Enter the chassis number as either 1 or 2.
active R0	Active instance in Route-processor slot 0.
standby R0	Standby instance in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see a summary of the AP upgrade information:

```
Device# show ap upgrade summary
```

show arp

To view the ARP table, use the **show arp** command.

show arp

Syntax Description

arp	Shows ARP table

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

The following example shows a sample output of the command:

```
Device# show arp

Address Age (min)     Hardware Addr
   9.11.8.1         0 84:80:2D:A0:D2:E6
9.11.32.111         0 3C:77:E6:02:33:3F
```

show arp summary

To see the ARP table summary, use the **show arp summary** command.

show arp summary

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the ARP table summary:

```
Device# show arp summary
```

show avc client

To display information about top number of applications, use the **show avc client** command in privileged EXEC mode.

show avc client *client-mac* **top** *n* **application** [**aggregate** | **upstream** | **downstream**]

Syntax Description

client *client-mac*	Specifies the client MAC address.
top *n* **application**	Specifies the number of top "N" applications for the given client.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following is sample output from the **show avc client** command:

```
Device# sh avc client 0040.96ae.65ec top 10 application aggregate

Cumulative Stats:

No.  AppName      Packet-Count    Byte-Count       AvgPkt-Size     usage%
---------------------------------------------------------------------------
1    skinny          7343           449860           61              94
2    unknown         99             13631            137             3
3    dhcp            18             8752             486             2
4    http            18             3264             181             1
5    tftp            9              534              59              0
6    dns             2              224              112             0

Last Interval(90 seconds) Stats:

No.  AppName     Packet-Count     Byte-Count       AvgPkt-Size      usage%
---------------------------------------------------------------------------
1    skinny          9              540              60               100
```

show avc wlan

To display information about top applications and users using the applications, use the **show avc wlan** command in privileged EXEC mode.

show avc wlan *ssid* **top** *n* **application** [**aggregate** | **upstream** | **downstream**]

Syntax Description

wlan *ssid*	Specifies the Service Set IDentifier (SSID) for WLAN.
top *n* **application**	Specifies the number of top "N" applications.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following is sample output from the **show avc wlan** command:

```
Device# show avc wlan Lobby_WLAN top 10 application aggregate

Cumulative Stats:

No.  AppName           Packet-Count          Byte-Count          AvgPkt-Size  usage%
-------------------------------------------------------------------------------------
1    ssl               10598677              1979525706            997          42
2    vnc               5550900               3764612847            678          14
3    http              3043131               2691327197            884          10
4    unknown           1856297               1140264956            614          4
5    video-over-http   1625019               2063335150            1269         8
6    binary-over-http  1329115               1744190344            1312         6
7    webex-meeting     1146872               540713787             471          2
8    rtp               923900                635650544             688          2
9    unknown           752341                911000213             1210         3
10   youtube           631085                706636186             1119         3

Last Interval(90 seconds) Stats:

No.  AppName          Packet-Count          Byte-Count           AvgPkt-Size  usage%
-------------------------------------------------------------------------------------
1    vnc               687093                602731844             877          68
2    video-over-http   213272                279831588             1312         31
3    ssl               6515                  5029365               771          1
4    webex-meeting     3649                  1722663               472          0
5    http              2634                  1334355               506          0
6    unknown           1436                  99412                 69           0
7    google-services   722                   378121                523          0
8    linkedin          655                   393263                600          0
9    exchange          432                   167390                387          0
10   gtalk-chat        330                   17330                 52           0
```

show chassis

To see the chassis information, use the **show chassis** command.

show chassis [{*1 2* | **detail** | **mode** | **neighbors** | **ha-status** {**active** | **local** | **standby**}}]

Syntax Description

{*1* | *2*}	Chassis number as 1 or 2 to see the information about the relevant chassis.
detail	Shows detailed information about the chassis.
mode	Shows information about the chassis mode.
neighbors	Shows information about the chassis neighbors.
ha-status	Option to see information about the High Availability (HA) status.
active	Shows HA status on the chassis that is in active state.
local	Shows HA status on the local .
standby	Shows HA status on the chassis that is in standby state.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the HA status on the active chassis:

```
Device# show chassis ha-status active
```

show checkpoint

To display information about the Checkpoint Facility (CF) subsystem, use the **show checkpoint** command.

show checkpoint { **clients** *client-ID <0-381>* | **entities***entity-ID <1-7>* | **statisticsbuffer-usage** }

Syntax Description

clients	Displays detailed information about checkpoint clients.
entities	Displays detailed information about checkpoint entities.
statistics	Displays detailed information about checkpoint statistics.
buffer-usage	Displays the checkpoint statistics of clients using large number of buffers.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
	This command was introduced.

This example shows how to display all the CF clients.

```
   Client residing in process  : 8135
------------------------------------------------------------------------------
Checkpoint client: WCM_MOBILITY
    Client ID                  : 24105
    Total DB inserts           : 0
    Total DB updates           : 0
    Total DB deletes           : 0
    Total DB reads             : 0
    Number of tables           : 6
    Client residing in process  : 8135
------------------------------------------------------------------------------
Checkpoint client: WCM_DOT1X
    Client ID                  : 24106
    Total DB inserts           : 2
    Total DB updates           : 1312
    Total DB deletes           : 2
    Total DB reads             : 0
    Number of tables           : 1
    Client residing in process  : 8135
------------------------------------------------------------------------------
Checkpoint client: WCM_APFROGUE
    Client ID                  : 24107
    Total DB inserts           : 0
    Total DB updates           : 0
    Total DB deletes           : 0
    Total DB reads             : 0
    Number of tables           : 1
    Client residing in process  : 8135
------------------------------------------------------------------------------
Checkpoint client: WCM_CIDS
    Client ID                  : 24110
    Total DB inserts           : 0
```

```
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 0
    Client residing in process  : 8135
------------------------------------------------------------------------------
Checkpoint client: WCM_NETFLOW
    Client ID                   : 24111
    Total DB inserts            : 7
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 1
    Client residing in process  : 8135
------------------------------------------------------------------------------
Checkpoint client: WCM_MCAST
    Client ID                   : 24112
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 1
    Client residing in process  : 8135
------------------------------------------------------------------------------
Checkpoint client: wcm_comet
    Client ID                   : 24150
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 0
    Client residing in process  : 8135
------------------------------------------------------------------------------

All iosd checkpoint clients

------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
Network RF Client           3         --       Off

  Total API Messages Sent:                      0
  Total Transport Messages Sent:                0
  Length of Sent Messages:                      0
  Total Blocked Messages Sent:                  0
  Length of Sent Blocked Messages:              0
  Total Non-blocked Messages Sent:              0
  Length of Sent Non-blocked Messages:          0
  Total Bytes Allocated:                        0
  Buffers Held:                                 0
  Buffers Held Peak:                            0
  Huge Buffers Requested:                       0
  Transport Frag Count:                         0
  Transport Frag Peak:                          0
  Transport Sends w/Flow Off:                   0
  Send Errs:                                    0
  Send Peer Errs:                               0
  Rcv Xform Errs:                               0
  Xmit Xform Errs:                              0
  Incompatible Messages:                        0
  Client Unbundles to Process Memory:           T
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
```

```
                            ID         ID       Mode
-------------------------------------------------------------------------------
SNMP CF Client              12         --       Off

  Total API Messages Sent:                        0
  Total Transport Messages Sent:                  0
  Length of Sent Messages:                        0
  Total Blocked Messages Sent:                    0
  Length of Sent Blocked Messages:                0
  Total Non-blocked Messages Sent:                0
  Length of Sent Non-blocked Messages:            0
  Total Bytes Allocated:                          0
  Buffers Held:                                   0
  Buffers Held Peak:                              0
  Huge Buffers Requested:                         0
  Transport Frag Count:                           0
  Transport Frag Peak:                            0
  Transport Sends w/Flow Off:                     0
  Send Errs:                                      0
  Send Peer Errs:                                 0
  Rcv Xform Errs:                                 0
  Xmit Xform Errs:                                0
  Incompatible Messages:                          0
  Client Unbundles to Process Memory:             T
-------------------------------------------------------------------------------
Client Name             Client     Entity     Bundle
                            ID         ID       Mode
-------------------------------------------------------------------------------
Online Diags HA             14         --       Off

  Total API Messages Sent:                        0
  Total Transport Messages Sent:                  0
  Length of Sent Messages:                        0
  Total Blocked Messages Sent:                    0
  Length of Sent Blocked Messages:                0
  Total Non-blocked Messages Sent:                0
  Length of Sent Non-blocked Messages:            0
  Total Bytes Allocated:                          0
  Buffers Held:                                   0
  Buffers Held Peak:                              0
  Huge Buffers Requested:                         0
  Transport Frag Count:                           0
  Transport Frag Peak:                            0
  Transport Sends w/Flow Off:                     0
  Send Errs:                                      0
  Send Peer Errs:                                 0
  Rcv Xform Errs:                                 0
  Xmit Xform Errs:                                0
  Incompatible Messages:                          0
  Client Unbundles to Process Memory:             T
-------------------------------------------------------------------------------
Client Name             Client     Entity     Bundle
                            ID         ID       Mode
-------------------------------------------------------------------------------
ARP                         22         --       Off

  Total API Messages Sent:                        0
  Total Transport Messages Sent:                  0
  Length of Sent Messages:                        0
  Total Blocked Messages Sent:                    0
  Length of Sent Blocked Messages:                0
  Total Non-blocked Messages Sent:                0
  Length of Sent Non-blocked Messages:            0
  Total Bytes Allocated:                          0
```

```
  Buffers Held:                                0
  Buffers Held Peak:                           0
  Huge Buffers Requested:                      0
  Transport Frag Count:                        0
  Transport Frag Peak:                         0
  Transport Sends w/Flow Off:                  0
  Send Errs:                                   0
  Send Peer Errs:                              0
  Rcv Xform Errs:                              0
  Xmit Xform Errs:                             0
  Incompatible Messages:                       0
  Client Unbundles to Process Memory:          T
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
Tableid CF                 27         --       Off

  Total API Messages Sent:                     0
  Total Transport Messages Sent:               0
  Length of Sent Messages:                     0
  Total Blocked Messages Sent:                 0
  Length of Sent Blocked Messages:             0
  Total Non-blocked Messages Sent:             0
  Length of Sent Non-blocked Messages:         0
  Total Bytes Allocated:                       0
  Buffers Held:                                0
  Buffers Held Peak:                           0
  Huge Buffers Requested:                      0
  Transport Frag Count:                        0
  Transport Frag Peak:                         0
  Transport Sends w/Flow Off:                  0
  Send Errs:                                   0
  Send Peer Errs:                              0
  Rcv Xform Errs:                              0
  Xmit Xform Errs:                             0
  Incompatible Messages:                       0
  Client Unbundles to Process Memory:          T
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
Event Manager              33          0       Off

  Total API Messages Sent:                     0
  Total Transport Messages Sent:               --
  Length of Sent Messages:                     0
  Total Blocked Messages Sent:                 0
  Length of Sent Blocked Messages:             0
  Total Non-blocked Messages Sent:             0
  Length of Sent Non-blocked Messages:         0
  Total Bytes Allocated:                       0
  Buffers Held:                                0
  Buffers Held Peak:                           0
  Huge Buffers Requested:                      0
  Transport Frag Count:                        0
  Transport Frag Peak:                         0
  Transport Sends w/Flow Off:                  0
  Send Errs:                                   0
  Send Peer Errs:                              0
  Rcv Xform Errs:                              0
  Xmit Xform Errs:                             0
  Incompatible Messages:                       0
  Client Unbundles to Process Memory:          T
```

```
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
LAN-Switch Port Mana       35          0       Off

  Total API Messages Sent:                      0
  Total Transport Messages Sent:                --
  Length of Sent Messages:                      0
  Total Blocked Messages Sent:                  0
  Length of Sent Blocked Messages:              0
  Total Non-blocked Messages Sent:              0
  Length of Sent Non-blocked Messages:          0
  Total Bytes Allocated:                        0
  Buffers Held:                                 0
  Buffers Held Peak:                            0
  Huge Buffers Requested:                       0
  Transport Frag Count:                         0
  Transport Frag Peak:                          0
  Transport Sends w/Flow Off:                   0
  Send Errs:                                    0
  Send Peer Errs:                               0
  Rcv Xform Errs:                               0
  Xmit Xform Errs:                              0
  Incompatible Messages:                        0
  Client Unbundles to Process Memory:           T
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
LAN-Switch PAgP/LACP       36          0       Off

  Total API Messages Sent:                      0
  Total Transport Messages Sent:                --
  Length of Sent Messages:                      0
  Total Blocked Messages Sent:                  0
  Length of Sent Blocked Messages:              0
  Total Non-blocked Messages Sent:              0
  Length of Sent Non-blocked Messages:          0
  Total Bytes Allocated:                        0
  Buffers Held:                                 0
  Buffers Held Peak:                            0
  Huge Buffers Requested:                       0
  Transport Frag Count:                         0
  Transport Frag Peak:                          0
  Transport Sends w/Flow Off:                   0
  Send Errs:                                    0
  Send Peer Errs:                               0
  Rcv Xform Errs:                               0
  Xmit Xform Errs:                              0
  Incompatible Messages:                        0
  Client Unbundles to Process Memory:           T
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
LAN-Switch VLANs           39          0       Off

  Total API Messages Sent:                      0
  Total Transport Messages Sent:                --
  Length of Sent Messages:                      0
  Total Blocked Messages Sent:                  0
  Length of Sent Blocked Messages:              0
  Total Non-blocked Messages Sent:              0
```

```
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
```

This example shows how to display all the CF entities.

```
KATANA_DOC#show checkpoint entities
                        Check Point List of Entities

 CHKPT on ACTIVE server.

------------------------------------------------------------------------------
Entity ID         Entity Name
------------------------------------------------------------------------------
        0         CHKPT_DEFAULT_ENTITY

  Total API Messages Sent:             0
  Total Messages Sent:                 0
  Total Sent Message Len:              0
  Total Bytes Allocated:               0
  Total Number of Members:            10

  Member(s) of entity 0 are:
    Client ID          Client Name
-----------------------------------------
          168          DHCP Snooping
          167          IGMP Snooping
           41          Spanning-tree
           40          AUTH MGR CHKPT CLIEN
           39          LAN-Switch VLANs
           33          Event Manager
           35          LAN-Switch Port Mana
           36          LAN-Switch PAgP/LACP
          158          Inline Power Checkpoint
```

This example shows how to display the CF statistics.

```
KATANA_DOC#show checkpoint statistics
        IOSd Check Point Status
 CHKPT on ACTIVE server.

Number Of Msgs In Hold Q:              0
CHKPT MAX Message Size:                0
TP MAX Message Size:               65503
CHKPT Pending Msg Timer:             100 ms

  FLOW_ON  total:                      0
  FLOW_OFF total:                      0
  Current FLOW status is:             ON
  Total API Messages Sent:             0
  Total Messages Sent:                 0
  Total Sent Message Len:              0
  Total Bytes Allocated:               0
  Rcv  Msg Q Peak:                     0
  Hold Msg Q Peak:                     0
```

```
Buffers Held Peak:                  0
Current Buffers Held:               0
Huge Buffers Requested:             0
```

show flow exporter

To display flow exporter status and statistics, use the **show flow exporter** command in privileged EXEC mode.

show flow exporter [{**export-ids netflow-v9** | [**name**] *exporter-name* [{**statistics** | **templates**}] | **statistics** | **templates**}]

Syntax Description

export-ids netflow-v9	(Optional) Displays the NetFlow Version 9 export fields that can be exported and their IDs.
name	(Optional) Specifies the name of a flow exporter.
exporter-name	(Optional) Name of a flow exporter that was previously configured.
statistics	(Optional) Displays statistics for all flow exporters or for the specified flow exporter.
templates	(Optional) Displays template information for all flow exporters or for the specified flow exporter.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following example displays the status and statistics for all of the flow exporters configured on a switch:

```
Device# show flow exporter
Flow Exporter FLOW-EXPORTER-1:
  Description:              Exports to the datacenter
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 192.168.0.1
    Source IP address:      192.168.0.2
    Transport Protocol:     UDP
    Destination Port:       9995
    Source Port:            55864
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Used
```

This table describes the significant fields shown in the display:

Table 9: show flow exporter Field Descriptions

Field	Description
Flow Exporter	The name of the flow exporter that you configured.

Field	Description
Description	The description that you configured for the exporter, or the default description User defined.
Transport Configuration	The transport configuration fields for this exporter.
Destination IP address	The IP address of the destination host.
Source IP address	The source IP address used by the exported packets.
Transport Protocol	The transport layer protocol used by the exported packets.
Destination Port	The destination UDP port to which the exported packets are sent.
Source Port	The source UDP port from which the exported packets are sent.
DSCP	The differentiated services code point (DSCP) value.
TTL	The time-to-live value.
Output Features	Specifies whether the **output-features** command, which causes the output features to be run on Flexible NetFlow export packets, has been used or not.

The following example displays the status and statistics for all of the flow exporters configured on a switch:

```
Device# show flow exporter name FLOW-EXPORTER-1 statistics
Flow Exporter FLOW-EXPORTER-1:
  Packet send statistics (last cleared 2w6d ago):
    Successfully sent:         0                     (0 bytes)
```

show flow interface

To display the configuration and status for an interface, use the **show flow interface** command in privileged EXEC mode.

show flow interface [*type number*]

Syntax Description

type	(Optional) The type of interface on which you want to display accounting configuration information.
number	(Optional) The number of the interface on which you want to display accounting configuration information.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Examples

The following example displays the accounting configuration on Ethernet interfaces 0/0 and 0/1:

```
Device# show flow interface gigabitethernet1/0/1

Interface Ethernet1/0
        monitor:         FLOW-MONITOR-1
        direction:       Output
        traffic(ip):     on
Device# show flow interface gigabitethernet1/0/2
Interface Ethernet0/0
        monitor:         FLOW-MONITOR-1
        direction:       Input
        traffic(ip):     sampler SAMPLER-2#
```

The table below describes the significant fields shown in the display.

Table 10: show flow interface Field Descriptions

Field	Description
Interface	The interface to which the information applies.
monitor	The name of the flow monitor that is configured on the interface.
direction:	The direction of traffic that is being monitored by the flow monitor. The possible values are: • Input—Traffic is being received by the interface. • Output—Traffic is being transmitted by the interface.

Field	Description
traffic(ip)	Indicates if the flow monitor is in normal mode or sampler mode. The possible values are: • on—The flow monitor is in normal mode. • sampler—The flow monitor is in sampler mode (the name of the sampler will be included in the display).

show flow monitor

To display the status and statistics for a flow monitor, use the **show flow monitor** command in privileged EXEC mode.

Syntax Description

name	(Optional) Specifies the name of a flow monitor.
monitor-name	(Optional) Name of a flow monitor that was previously configured.
cache	(Optional) Displays the contents of the cache for the flow monitor.
format	(Optional) Specifies the use of one of the format options for formatting the display output.
csv	(Optional) Displays the flow monitor cache contents in comma-separated variables (CSV) format.
record	(Optional) Displays the flow monitor cache contents in record format.
table	(Optional) Displays the flow monitor cache contents in table format.
statistics	(Optional) Displays the statistics for the flow monitor.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

The **cache** keyword uses the record format by default.

The uppercase field names in the display output of the **show flowmonitor** *monitor-name* **cache** command are key fields that uses to differentiate flows. The lowercase field names in the display output of the **show flow monitor** *monitor-name* **cache** command are nonkey fields from which collects values as additional data for the cache.

Examples

The following example displays the status for a flow monitor:

```
Device# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       Used for basic traffic analysis
  Flow Record:       flow-record-1
  Flow Exporter:     flow-exporter-1
                     flow-exporter-2
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 311316 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
```

This table describes the significant fields shown in the display.

Table 11: show flow monitor monitor-name Field Descriptions

Field	Description
Flow Monitor	Name of the flow monitor that you configured.
Description	Description that you configured or the monitor, or the default description User defined.
Flow Record	Flow record assigned to the flow monitor.
Flow Exporter	Exporters that are assigned to the flow monitor.
Cache	Information about the cache for the flow monitor.
Type	Flow monitor cache type. The value is always normal, as it is the only supported cache type.
Status	Status of the flow monitor cache. The possible values are: • allocated—The cache is allocated. • being deleted—The cache is being deleted. • not allocated—The cache is not allocated.
Size	Current cache size.
Inactive Timeout	Current value for the inactive timeout in seconds.
Active Timeout	Current value for the active timeout in seconds.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1:

This table describes the significant fields shown in the display.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1 in a table format:

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-IPv6 (the cache contains IPv6 data) in record format:

The following example displays the status and statistics for a flow monitor:

show flow record

To display the status and statistics for a flow record, use the **show flow record** command in privileged EXEC mode.

show flow record [{[**name**] *record-name*}]

Syntax Description

name	(Optional) Specifies the name of a flow record.
record-name	(Optional) Name of a user-defined flow record that was previously configured.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following example displays the status and statistics for FLOW-RECORD-1:

```
Device# show flow record FLOW-RECORD-1
flow record FLOW-RECORD-1:
  Description:        User defined
  No. of users:       0
  Total field space:  24 bytes
  Fields:
    match ipv6 destination address
    match transport source-port
    collect interface input
```

show interfaces

To display the administrative and operational status of all interfaces or for a specified interface, use the **show interfaces** command in privileged EXEC mode.

show interfaces [{*interface-id* | **vlan** *vlan-id*}] [{**accounting** | **capabilities** [**module** *number*] | **debounce** | **description** | **etherchannel** | **flowcontrol** | **private-vlan mapping** | **pruning** | **stats** | **status** [{**err-disabled**}] | **trunk**}]

Syntax Description

interface-id	(Optional) ID of the interface. Valid interfaces include physical ports (including type, stack member , module, and port number) and port channels. The port channel range is 1 to 48.
vlan *vlan-id*	(Optional) VLAN identification. The range is 1 to 4094.
accounting	(Optional) Displays accounting information on the interface, including active protocols and input and output packets and octets. **Note** The display shows only packets processed in software; hardware-switched packets do not appear.
capabilities	(Optional) Displays the capabilities of all interfaces or the specified interface, including the features and options that you can configure on the interface. Though visible in the command line help, this option is not available for VLAN IDs.
module *number*	(Optional) Displays capabilities of all interfaces on the switch or specified stack member. This option is not available if you entered a specific interface ID.
description	(Optional) Displays the administrative status and description set for an interface.
etherchannel	(Optional) Displays interface EtherChannel information.
flowcontrol	(Optional) Displays interface flow control information.
private-vlan mapping	(Optional) Displays private-VLAN mapping information for the VLAN switch virtual interfaces (SVIs). This keyword is not available if the switch is running the LAN base feature set.
pruning	(Optional) Displays trunk VTP pruning information for the interface.
stats	(Optional) Displays the input and output packets by switching the path for the interface.
status	(Optional) Displays the status of the interface. A status of unsupported in the Type field means that a non-Cisco small form-factor pluggable (SFP) module is inserted in the module slot.

err-disabled	(Optional) Displays interfaces in an error-disabled state.
trunk	(Optional) Displays interface trunk information. If you do not specify an interface, only information for active trunking ports appears.

Note Though visible in the command-line help strings, the **crb**, **fair-queue**, **irb**, **mac-accounting**, **precedence**, **random-detect**, **rate-limit**, and **shape** keywords are not supported.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines The **show interfaces capabilities** command with different keywords has these results:

- Use the **show interface capabilities module** *number* command to display the capabilities of all interfaces on that in the stack. If there is no with that module number in the stack, there is no output.
- Use the **show interfaces** *interface-id* **capabilities** to display the capabilities of the specified interface.
- Use the **show interfaces capabilities** (with no module number or interface ID) to display the capabilities of all interfaces in the stack.

This is an example of output from the **show interfaces** command for an interface on stack member 3:

```
Device#show interfaces gigabitEthernet 0
GigabitEthernet0 is up, line protocol is up
Hardware is MEWLC management port, address is 0000.5e00.0101 (bia 0000.0000.0000)
Internet address is 20.61.1.12/16
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Unknown, Unknown, media type is unknown media type
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 03:06:36, output 00:00:07, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
0 packets output, 0 bytes, 0 underruns
```

```
0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
```

This is an example of output from the **show interfaces** *interface* **description** command when the interface has been described as *Connects to Marketing* by using the **description** interface configuration command:

```
Device# show interfaces gigabitethernet1/0/2 description
Interface                      Status         Protocol Description
Gi1/0/2                        up             down     Connects to Marketing
```

This is an example of output from the **show interfaces** *interface-id* **pruning** command when pruning is enabled in the VTP domain:

```
Device# show interfaces gigabitethernet1/0/2 pruning
Port      Vlans pruned for lack of request by neighbor
Gi1/0/2   3,4

Port      Vlans traffic requested of neighbor
Gi1/0/2   1-3
```

This is an example of output from the **show interfaces stats** command for a specified VLAN interface:

```
Device# show interfaces vlan 1 stats
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
     Processor    1165354   136205310      570800     91731594
   Route cache          0           0           0            0
         Total    1165354   136205310      570800     91731594
```

These are examples of output from the **show interfaces status** command for a specific interface when private VLANs are configured. Port 22 is configured as a private-VLAN host port. It is associated with primary VLAN 20 and secondary VLAN 25:

```
Device# show interfaces gigabitethernet1/0/22 status
Port       Name      Status      Vlan      Duplex      Speed      Type
Gi1/0/22             connected   20,25     a-full      a-100      10/100BaseTX
```

In this example, port 20 is configured as a private-VLAN promiscuous port. The display shows only the primary VLAN 20:

```
Device# show interfaces gigabitethernet1/0/20 status
Port       Name      Status      Vlan      Duplex      Speed      Type
Gi1/0/20             connected   20        a-full      a-100      10/100BaseTX
```

This is an example of output from the **show interfaces status err-disabled** command. It displays the status of interfaces in the error-disabled state:

```
Device# show interfaces status err-disabled
Port      Name       Status         Reason
Gi1/0/2              err-disabled   gbic-invalid
Gi2/0/3              err-disabled   dtp-flap
```

This is an example of output from the **show interfaces** *interface-id* **pruning** command:

```
Device# show interfaces gigabitethernet1/0/2 pruning
Port Vlans pruned for lack of request by neighbor
```

```
Device# show interfaces gigabitethernet1/0/1 trunk
Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/1     on               802.1q         other         10

Port        Vlans allowed on trunk
Gi1/0/1     none

Port        Vlans allowed and active in management domain
Gi1/0/1     none

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/1     none
```

show install package

To view the install package details, use the **show install package** command.

show install package

Syntax Description

This command has no arguments.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

Example

This example shows how to view the install package details:

```
Device#show install package
```

show install rollback

To view the package information for a rollback point, use the **show install rollback** command.

show install rollback

Syntax Description

This command has no arguments.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

Example

This example shows how to view the package information for a rollback point:

```
Device#show install rollback
```

show install summary

To view the install manager summary, use the **show install summary** command.

show install summary

Syntax Description

This command has no arguments.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

Example

This example shows how to view the install summary information:

```
Device#show install summary
```

show ip

To view the IP information, use the **show ip** command.

Syntax Description

access-lists	Lists the IP access lists
interface	Displays the IP interface status and configuration
brief	Displays the brief summary of IP status and configuration
route	Displays the IP routing table
tunnel	Displays the IP tunnel information
eogre	Displays the EoGRE tunnel information
domain	Displays the EoGRE tunnel domain information
forwarding-table	Displays the EoGRE tunnel encapsulation and decapsulation information
gateway	Displays the EoGRE tunnel gateway information
fabric	Displays the IP fabric tunnel information
summary	Displays the information for all tunnels

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view information about the lists the IP access lists:

```
cisco-wave2-ap# show ip access-lists
```

show ip nbar protocol-id

To see NBAR protocol classification ID, use the **show ip nbar protocol-id** command.

show ip nbar protocol-id name

Syntax Description

protocol-id	The protocol classification ID.
name	Host server name

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Examples

The following example shows how to see the NBAR protocol classification ID:

```
Device# show ip nbar protocol-id name
```

show ldap attributes

To view information about the default LDAP attribute mapping, use the **show ldap attributes** command.

show ldap attributes

Syntax Description

This command has no arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to view information about the default LDAP attribute mapping:

```
Device# show ldap attributes
LDAP Attribute                  Format     AAA Attribute
==============                  ======     =============
airespaceBwDataBurstContract    Ulong      bsn-data-bandwidth-burst-contr
userPassword                    String     password
airespaceBwRealBurstContract    Ulong      bsn-realtime-bandwidth-burst-c
employeeType                    String     employee-type
airespaceServiceType            Ulong      service-type
airespaceACLName                String     bsn-acl-name
priv-lvl                        Ulong      priv-lvl
memberOf                        String DN  supplicant-group
cn                              String     username
airespaceDSCP                   Ulong      bsn-dscp
policyTag                       String     tag-name
airespaceQOSLevel               Ulong      bsn-qos-level
airespace8021PType              Ulong      bsn-8021p-type
airespaceBwRealAveContract      Ulong      bsn-realtime-bandwidth-average
airespaceVlanInterfaceName      String     bsn-vlan-interface-name
airespaceVapId                  Ulong      bsn-wlan-id
airespaceBwDataAveContract      Ulong      bsn-data-bandwidth-average-con
sAMAccountName                  String     sam-account-name
meetingContactInfo              String     contact-info
telephoneNumber                 String     telephone-number
Map: att_map_1
department                      String DN  element-req-qos
```

show ldap server

To view the LDAP server state information and various other counters for the server, use the **show ldap server** command.

show ldap server

Syntax Description

This command has no arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to view the LDAP server state information and various other counters for the server:

```
Device# show ldap server
```

show license all

To display all licensing information enter the **show license all** command in Privileged EXEC mode. This command displays status, authorization, UDI, and usage information, all combined.

show license all

Syntax Description

This command has no keywords or arguments

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to display information relating to Smart Licensing Using Policy. Command output no longer displays Smart Account and Virtual account information.

Usage Guidelines

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2 or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Example (Smart Licensing Using Policy)

The following is sample output of the **show license all** command on a Cisco Catalyst 9800-CL Wireless Controller. Similar output is displayed on all supported Cisco Catalyst Wireless Controllers.

```
Device# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED
License Reservation is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
```

```
  Version privacy: DISABLED

Transport:
  Type: Transport Off

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: Nov 01 20:31:46 2020 IST
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

License Usage
=============

air-network-advantage (DNA_NWStack):
  Description: air-network-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-network-advantage
  Feature Description: air-network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20

air-dna-advantage (AIR-DNA-A):
  Description: air-dna-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-dna-advantage
  Feature Description: air-dna-advantage
```

```
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20

Product Information
===================
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS

HA UDI List:
    Active:PID:C9800-CL-K9,SN:93BBAH93MGS
    Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN

Agent Version
=============
Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations
======================
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
      Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      Last Confirmation code: ad4382fe

Specified license reservations:
  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
    Description: DNA Advantage for Wireless
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10
  AP Perpetual Networkstack Advantage (DNA_NWStack):
    Description: AP Perpetual Network Stack entitled with DNA-A
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
```

```
            Start Date: 2020-JUN-18 UTC
            End Date: 2020-DEC-15 UTC
            Term Count: 5
        Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
          Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
          License type: TERM
            Start Date: 2020-OCT-14 UTC
            End Date: 2021-APR-12 UTC
            Term Count: 10

Purchased Licenses:
  No Purchase Information Available
```

show license authorization

To display authorization-related information for (export-controlled and enforced) licenses, enter the **show license authorization** command in privileged EXEC mode.

show license authorization

Syntax Description

This command has no keywords or arguments

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	This command was introduced.

Usage Guidelines

Only export-controlled or enforced licenses require authorization before use.

While there are no export-controlled or enforced licenses on Cisco Catalyst Wireless Controllers, you can use this command to display migrated SLR authorization codes.

Examples

See Table 12: show license authorization Field Descriptions, on page 632 for information about fields shown in the display.

See show license authorization Displaying Migrated Authorization Code, on page 634 for sample output.

Table 12: show license authorization Field Descriptions

Field		Description
Overall Status	Header for UDI information for all product instances in the set-up, the type of authorization that is installed, and configuration errors, if any. In a High Availability set-up, all UDIs in the set-up are listed.	
	Active: Status:	The active product instance UDI, followed by the status of the authorization code installation for this UDI. If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.
	Standby: Status:	The standby product instance UDI, followed by the status of the authorization code installation for this UDI. If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.
	Member: Status:	The member product instance UDI, followed by the status of the authorization code installation for this UDI. If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.
	ERROR:	Configuration errors or discrepancies in the High Availability set-up, if any.

Field		Description
Authorizations	Header for detailed license authorization information. All licenses, their enforcement types, and validity durations are displayed. Errors are displayed for each product instance if its authorization or mode does not match what is installed on the active. This section is displayed only if the product instance is using a license with an authorization code.	
	():	License name and a shortened form of the license name.
	Description	License description.
	Total available count:	Total count of licenses that are available to consume. This includes licenses of all durations (perpetual and subscription), including expired subscription licenses, for all the product instances in a High Availability setup.
	Enforcement type	Enforcement type for the license. This may be one of the following: • Enforced • Not enforced • Export-Controlled
	Term information:	

Field		Description
		Header providing license duration information. The following fields maybe included under this header: • Active: The active product instance UDI, followed by the status of the authorization code installation for this UDI. • Authorization type: Type of authorization code installed and date of installation. The type can be: SLAC, UNIVERSAL, SPECIFIED, PAK, RTU. • Start Date: Displays validity start date if the license is for a specific term or time period. • Start Date: Displays validity end date if the license is for a specific term or time period. • Term Count: License count. • Subscription ID: Displays ID if the license is for a specific term or time period. • License type: License duration. This can be: SUBSCRIPTION or PERPETUAL. • Standby: The standby product instance UDI, followed by the status of the authorization code installation for this UDI. • Member: The member product instance UDI, followed by the status of the authorization code installation for this UDI. For more information about the duration or term of a license's validity, see <link tbd>.
Purchased Licenses	Header for license purchase information.	
	Active:	The active product instance and its the UDI.
	Count:	License count.
	Description:	License description.
	License type:	License duration. This can be: SUBSCRIPTION or PERPETUAL.
	Standby:	The standby product instance UDI.
	Member:	The member product instance UDI.

show license authorization Displaying Migrated Authorization Code

The following is sample output of the **show license authorization** command on a Cisco Catalyst 9800-CL Wireless Controller. The `Last Confirmation code:` shows that SLR authorization code is available after migration. Similar output is displayed on all supported Cisco Catalyst Wireless Controllers.

```
Device# show license authorization
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
      Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      Last Confirmation code: ad4382fe

Specified license reservations:
  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
    Description: DNA Advantage for Wireless
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10
  AP Perpetual Networkstack Advantage (DNA_NWStack):
    Description: AP Perpetual Network Stack entitled with DNA-A
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10

Purchased Licenses:
  No Purchase Information Available
```

show license data conversion

To display license data conversion information, enter the **show license data** command in privileged EXEC mode.

show license data conversion

Syntax Description

This command has no keywords or arguments

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	This command continues to be available with the introduction of Smart Licensing Using Policy.

Usage Guidelines

Although visible on the CLI, this command is not applicable to Cisco Catalyst Wireless Controllers.

show license eventlog

To display event logs relating to Smart Licensing Using Policy, enter the **show license eventlog** command in privileged EXEC mode.

show license eventlog [*days*]

Syntax Description

days	Enter the number of days for which you want to display event logs. The valid value range is from 0 to 2147483647.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Additional events were added with the introduction of Smart Licensing Using Policy: • Installation and removal of a policy • Request, installation and removal of an authorization code. • Installation and removal of a trust code. • Addition of authorization source information for license usage.

Usage Guidelines

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

show license history message

To display communication history between the product instance and CSSM or CSLU (as the case may be), enter the **show license history message** command in privileged EXEC mode. The output of this command is used by the technical support team, for troubleshooting.

show license history message

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	This command was introduced.

Usage Guidelines

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra** privileged EXEC commands.

show license reservation

To display license reservation information, enter the **show license reservation** command in privileged EXEC mode.

show license reservation

Syntax Description

This command has no keywords or arguments

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	This command continues to be available with the introduction of Smart Licensing Using Policy.

Usage Guidelines

The command continues to be available on the CLI and corresponding output is displayed, but with the introduction of Smart Licensing Using Policy, the notion of reservation is not longer applicable. Use the **show license all** command in privileged EXEC mode, to display *migrated* SLR licenses instead (the SLR authorization code is migrated to Smart Licensing Using Policy).

show license status

To display information about licensing settings such as data privacy, policy, transport, usage reporting and trust codes, enter the **show license status** command in privileged EXEC mode.

show license status

Syntax Description

This command has no keywords or arguments

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy. This includes `Trust code installed:`, `Policy in use`, `Policy name:` , reporting requirements as in the policy (`Attributes:`), and fields related to usage reporting. Command output no longer displays Smart Account and Virtual account information.

Usage Guidelines

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Examples

See Table 13: show license status Field Descriptions for Smart Licensing Using Policy, on page 641 for information about fields shown in the display.

show license status with Cisco Default Policy (Smart Licensing Using Policy), on page 646

show license status with Custom Policy (Smart Licensing Using Policy), on page 647

Table 13: show license status Field Descriptions for Smart Licensing Using Policy

Field		Description
Utility	Header for utility settings that are configured on the product instance.	
	Status:	Status
	Utility report:	Last attempt:
	Customer Information:	The following fields are displayed: • Id: • Name: • Street • City: • State: • Country: • Postal Code:
Smart Licensing Using Policy:	Header for policy settings on the product instance.	
	Status:	Indicates if Smart Licensing Using Policy is enabled. Smart Licensing Using Policy is supported starting from Cisco IOS XE Amsterdam 17.3.2 and is always enabled on supported software images.
Data Privacy:	Header for privacy settings that are configured on the product instance.	
	Sending Hostname:	A *yes* or *no* value which shows if the hostname is sent in usage reports.
	Callhome hostname privacy:	Indicates if the Call Home feature is configured as the mode of transport for reporting. If configured, one of these values is displayed: • ENABLED • DISABLED
	Smart Licensing hostname privacy:	One of these values is displayed: • ENABLED • DISABLED
	Version privacy:	One of these values is displayed: • ENABLED • DISABLED

Field		Description
Transport:	Header for transport settings that are configured on the product instance.	
	Type:	Mode of transport that is in use. Additional fields are displayed for certain transport modes. For example, if transport type is set to CSLU, the CSLU address is also displayed.

Field		Description
Policy:	Header for policy information that is applicable to the product instance.	
	Policy in use:	Policy that is applied This can be one of the following: Cisco default, Product default, Permanent License Reservation, Specific License Reservation, PAK license, Installed on <date>, Controller.
	Policy name:	Name of the policy
	Reporting ACK required:	A *yes* or *no* value which specifies if the report for this product instance requires CSSM acknowledgement (ACK) or not. The default policy is always set to "yes".
	Unenforced/Non-Export Perpetual Attributes	Displays policy values for perpetual licenses. • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): he maximum amount of time available to send a report in case of a change in license usage, followed by policy name
	Unenforced/Non-Export Subscription Attributes	Displays policy values for subscription licenses. • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): he maximum amount of time available to send a report in case of a change in license usage, followed by policy name
	Enforced (Perpetual/Subscription) License Attributes	

Field		Description
		Displays policy values for enforced licenses. • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): The maximum amount of time available to send a report in case of a change in license usage, followed by policy name
	Export (Perpetual/Subscription) License Attributes	Displays policy values for export-controlled licenses. • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): The maximum amount of time available to send a report in case of a change in license usage, followed by policy name
Miscellaneous	Header for custom ID.	
	Custom Id:	ID

Field		Description
Usage Reporting:	Header for usage reporting (RUM reports) information.	
	Last ACK received:	Date and time of last ACK received, in the local time zone.
	Next ACK deadline:	Date and time for next ACK. If the policy states that an ACK is not requires then this field displays `none`. **Note** If an ACK is required and is not received by this deadline, a syslog is displayed.
	Reporting Interval:	Reporting interval in days The value displayed here depends on what you configure in the **license smart usage interval***interval_in_days* and the policy value. For more information, see the corresponding Syntax Description: license smart (global config), on page 320.
	Next ACK push check:	Date and time when the product instance will submit the next polling request for an ACK. Date and time are in the local time zone. This applies only to product instance- initiated communication to CSSM or CSLU. If the reporting interval is zero, or if no ACK polling is pending, then this field displays `none`.
	Next report push:	Date and time when the product instance will send the next RUM report. Date and time are in the local time zone. If the reporting interval is zero, or if there are no pending RUM reports, then this field displays `none`.
	Last report push:	Date and time for when the product instance sent the last RUM report. Date and time are in the local time zone.
	Last report file write:	Date and time for when the product instance last saved an offline RUM report. Date and time are in the local time zone.
	Last report pull:	Date and time for when usage reporting information was retrieved using data models. Date and time are in the local time zone.

Field		Description
Trust Code Installed:	Header for trust code-related information. Displays date and time if trust code is installed. Date and time are in the local time zone. If a trust code is not installed, then this field displays `none`.	
	Active:	Active product instance. In a High Availability set-up, the the UDIs of all product instances in the set-up, along with corresponding trust code installation dates and times are displayed.
	Standby:	Standby product instance.
	Member:	Member product instance

show license status with Cisco Default Policy (Smart Licensing Using Policy)

The following is sample output of the **show license status** command; a default is policy applied here.

```
Device# show license status

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
```

```
    Report on change (days): 0 (CISCO default)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>
```

show license status with Custom Policy (Smart Licensing Using Policy)

The following is sample output of the **show license status** command; a custom policy applied here.

```
Device# show license status
Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured

Policy:
  Policy in use: Installed On Nov 02 05:09:31 2020 IST
  Policy name: SLE Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 60 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>
```

```
Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
    INSTALLED on Nov 02 05:09:31 2020 IST
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
    INSTALLED on Nov 02 05:09:31 2020 IST
```

show license summary

To display a brief summary of license usage, which includes information about licenses being used, the count, and status, enter the **show license summary** command in privileged EXEC mode.

show license summary

Syntax Description

This command has no keywords or arguments

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect valid license status for Smart Licensing Using Policy. Valid license statuses include: `IN USE`, `NOT IN USE`, `NOT AUTHORIZED`. Command output was also updated to remove registration and authorization information. Command output no longer displays Smart Account and Virtual account information.

Usage Guidelines

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

The licenses on Cisco Catalyst Wireless Controllers are never `NOT AUTHORIZED`, because none of the available licenses are export-controlled or enforced (Only these licenses require authorization before use).

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Examples

See Table 14: show license summary Field Descriptions, on page 649 for information about fields shown in the display.

show license summary: IN USE (Smart Licensing Using Policy), on page 650

show license summary: NOT IN USE (Smart Licensing Using Policy), on page 650

Table 14: show license summary Field Descriptions

Field	Description
License	Name of the licenses in use
Entitlement Tag	Short name for license
Count	License count

Field	Description
Status	License status can be one of the following • In-Use: Valid license, and in-use. • Not In-Use • Not Authorized: Means that the license requires installation of SLAC before use.

show license summary: IN USE (Smart Licensing Using Policy)

The following is sample output of the **show license summary** command where all licenses are in-use.

```
Devide# show license summary

License Usage:
  License                Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  air-network-essentials  (DNA_NWSTACK_E)                  1 IN USE
  air-dna-essentials      (AIR-DNA-E)                      1 IN USE
```

show license summary: NOT IN USE (Smart Licensing Using Policy)

The following is sample output of the **show license summary** command, where none of the APs have joined the controller. Current consumption (Count) is therefore zero, and the `Status` field shows that the licenses are `NOT IN USE`:

```
Device# show license summary

Device#show license summary
License Reservation is ENABLED

License Usage:
  License                Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  Aironet DNA Advantag... (AIR-DNA-A)                      0 NOT IN USE
  AP Perpetual Network... (DNA_NWStack)                    0 NOT IN USE
```

show license tech

To display licensing information to help the technical support team to solve a problem, enter the **show license tech** command in privileged EXEC mode. The output for this command includes outputs of several other **show license** commands and more.

show license tech { **data** { **conversion** } | **eventlog** [{ *days* }] | **reservation** | **support** }

Syntax Description

data { **conversion** }	Displays license data conversion information.
eventlog [{ *days* }]	Displays event logs related to Smart Licensing Using Policy. For *days*, enter the number of days for which you want to display event logs. The valid value range is from 0 to 2147483647.
reservation	Displays license reservation information.
support	Displays licensing information that helps the technical support team to debug a problem.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy.

Usage Guidelines

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra all** privileged EXEC commands.

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing (whether smart licensing is enabled, all associated licensing certificates, compliance status, and so on).

Example (Smart Licensing Using Policy)

The following is sample output from the **show license tech support** command.

```
Device# show license tech support

Smart Licensing Tech Support info

Smart Licensing Status
======================

Smart Licensing is ENABLED
```

```
License Reservation is ENABLED

Registration:
  Status: REGISTERED - SPECIFIC LICENSE RESERVATION
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Nov 02 03:16:01 2020 IST

License Authorization:
  Status: AUTHORIZED - RESERVED on Nov 02 03:16:01 2020 IST

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license

Evaluation Period:
  Evaluation Mode: Not In Use
  Evaluation Period Remaining: 89 days, 23 hours, 42 minutes, 47 seconds

License Usage
=============
Handle: 1
  License: AP Perpetual Networkstack Advantage
  Entitlement tag:
regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896
  Description: AP Perpetual Network Stack entitled with DNA-A
  Count: 1
  Version: 1.0
  Status: AUTHORIZED(3)
  Status time: Nov 02 03:16:01 2020 IST
  Request Time: Nov 02 02:55:34 2020 IST
  Export status: NOT RESTRICTED
  Soft Enforced: True

Handle: 2
  License: Aironet DNA Advantage Term Licenses
  Entitlement tag: regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790

  Description: DNA Advantage for Wireless
  Count: 1
  Version: 1.0
  Status: AUTHORIZED(3)
  Status time: Nov 02 03:16:01 2020 IST
  Request Time: Nov 02 02:55:34 2020 IST
  Export status: NOT RESTRICTED
  Soft Enforced: True

Product Information
===================
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS

HA UDI List:
```

```
    Active:PID:C9800-CL-K9,SN:93BBAH93MGS
    Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN

Agent Version
=============
Smart Agent for Licensing: 4.8.7_rel/52

Upcoming Scheduled Jobs
=======================
Current time: Nov 02 03:17:23 2020 IST
Daily: Nov 03 02:47:04 2020 IST (23 hours, 29 minutes, 41 seconds remaining)
Certificate Renewal: Not Available
Certificate Expiration Check: Not Available
Authorization Renewal: Not Available
Authorization Expiration Check: Not Available
Init Flag Check: Not Available
Evaluation Expiration Check: Not Available
Ack Expiration Check: Not Available
Evaluation Expiration Warning: Not Available
IdCert Expiration Warning: Not Available
Reservation request in progress warning: Not Available
Reservation configuration mismatch between nodes in HA mode: Nov 09 03:16:30 2020 IST (6
days, 23 hours, 59 minutes, 7 seconds remaining)
Endpoint Report Request: Not Available

License Certificates
====================
Production Cert: True
Not registered. No certificates installed

HA Info
==========
RP Role: Active
Chassis Role: Active
Behavior Role: Active
RMF: True
CF: True
CF State: Stateless
Message Flow Allowed: False

Reservation Info
================
License reservation: ENABLED

Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Reservation status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
      Export-Controlled Functionality: ALLOWED
      Request code: <none>
      Last return code: <none>
      Last Confirmation code: 102fc949
      Reservation authorization code:
<specificPLR><authorizationCode><flag>A</flag><version>C</version><piid>e913b4787a742a5791</piid><timestamp>1604298710</timestamp><entitlements><entitlement><tag>regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6387a0-41a-a3958a1b79</tag><count>5</count><startDate>2020-Oct-14
 UTC</startDate><endDate>2021-Apr-12
UTC</endDate><licenseType>TERM</licenseType><displayName>Aironet DNA Advantage Term
Licenses</displayName><tagDescription>DNA Advantage for
Wireless</tagDescription><subscriptionID></subscriptionID></entitlement><entitlement><tag>regid.2017-08.com.cisco.AIR-DNA-A,1.0_b63867-3a10-4a11-a3d9-5691a0d793</tag><count>5</count><startDate>2020-Jun-18
 UTC</startDate><endDate>2020-Dec-15
UTC</endDate><licenseType>TERM</licenseType><displayName>Aironet DNA Advantage Term
Licenses</displayName><tagDescription>DNA Advantage for
Wireless</tagDescription><subscriptionID></subscriptionID></entitlement><entitlement><tag>regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3a05-4608-8bf0-d12f67808996</tag><count>5</count><startDate>2020-Oct-14
 UTC</startDate><endDate>2021-Apr-12
UTC</endDate><licenseType>TERM</licenseType><displayName>AP Perpetual Networkstack
Advantage</displayName><tagDescription>AP Perpetual Network Stack entitled with
```

```
DNA-A</tagDescription><subscriptionID></subscriptionID></entitlement><entitlement><tag>regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896</tag><count>5</count><startDate>2020-Jun-18
 UTC</startDate><endDate>2020-Dec-15
UTC</endDate><licenseType>TERM</licenseType><displayName>AP Perpetual Networkstack
Advantage</displayName><tagDescription>AP Perpetual Network Stack entitled with
DNA-A</tagDescription><subscriptionID></subscriptionID></entitlement></entitlements></authorizationCode><signature>[illegible]</signature><udi>P:C9800-CL-K9,S:93BBAH93MGS</udi></specificPLR>

  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Reservation status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      Export-Controlled Functionality: ALLOWED
      Request code: <none>
      Last return code: <none>
      Last Confirmation code: ad4382fe
      Reservation authorization code:
<specificPLR><authorizationCode><flag>A</flag><version>C</version><piid>[illegible]</piid><timestamp>[illegible]</timestamp><entitlements><entitlement><tag>regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896</tag><count>10</count><startDate>2020-Oct-14
 UTC</startDate><endDate>2021-Apr-12
UTC</endDate><licenseType>TERM</licenseType><displayName>AP Perpetual Networkstack
Advantage</displayName><tagDescription>AP Perpetual Network Stack entitled with
DNA-A</tagDescription><subscriptionID></subscriptionID></entitlement><entitlement><tag>regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-5d691a0d7913</tag><count>10</count><startDate>2020-Oct-14
 UTC</startDate><endDate>2021-Apr-12
UTC</endDate><licenseType>TERM</licenseType><displayName>Aironet DNA Advantage Term
Licenses</displayName><tagDescription>DNA Advantage for
Wireless</tagDescription><subscriptionID></subscriptionID></entitlement></entitlements></authorizationCode><signature>[illegible]</signature><udi>P:C9800-CL-K9,S:9XECPSUU4XN</udi></specificPLR>

Specified license reservations:
  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
    Description: DNA Advantage for Wireless
    Total reserved count: 20
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
          Subscription ID: <none>
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
          Subscription ID: <none>
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10
          Subscription ID: <none>
  AP Perpetual Networkstack Advantage (DNA_NWStack):
    Description: AP Perpetual Network Stack entitled with DNA-A
    Total reserved count: 20
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
          Subscription ID: <none>
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
          Subscription ID: <none>
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
```

```
          Term Count: 10
          Subscription ID: <none>

Other Info
==========
Software ID: regid.2018-05.com.cisco.WLC_9500C,1.0_85665885-b865-4e32-8184-5510412fcb54
Agent State: authorized
TS enable: True
Transport: Smart
  Default URL: https://smartreceiver.cisco.com/licservice/license
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True
Privacy Send IP: True
Build type:: Production
sizeof(char)  : 1
sizeof(int)   : 4
sizeof(long)  : 4
sizeof(char *): 8
sizeof(time_t): 4
sizeof(size_t): 8
Endian: Big
Write Erase Occurred: False
XOS version: 0.12.0.0
Config Persist Received: False
Message Version: 1.3
connect_info.name: <empty>
connect_info.version: <empty>
connect_info.additional: <empty>
connect_info.prod: False
connect_info.capabilities: <empty>
agent.capabilities: UTILITY, DLC, AppHA, MULTITIER, EXPORT_2, OK_TRY_AGAIN
SmartAgentClientWaitForServer: 2000
SmartAgentCmReTrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
SmartAgentFederalLicense: True
SmartAgent_Crypto_Exit_CB: 0x55B353357A20
SmartAgent_Crypto_Start_CB: 0x55B353357A10
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
SmartAgentDelayCertValidation: False
enableByDefault: False
conversionAutomatic: True
conversionAllowed: False
storageEncryptDisable: False
storageLoadUnencryptedDisable: False
TSPluginDisable: False
bypassUDICheck: False
loggingAddTStamp: False
loggingAddTid: True
platformOverrideEvent: UnknownPlatformEvent
WaitForHaRole: False
standbyIsHot: True
chkPtType: 2
delayCommInit: False
roleByEvent: True
maxTraceLength: 150
```

```
traceAlwaysOn: True
debugFlags: 0
Event log max size: 5120 KB
Event log current size: 21 KB

Platform Provided Mapping Table
===============================
<empty>
```

show license udi

To display Unique Device Identifier (UDI) information for a product instance, enter the **show license udi** command in privileged EXEC mode. In a High Availability set-up, the output displays UDI information for all connected product instances.

show license udi

Syntax Description

This command has no keywords or arguments

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	This command continues to be available with the introduction of Smart Licensing Using Policy.

Usage Guidelines

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Examples

show license udi with Standalone Product Instance, on page 657

show license udi with Active and Standby, on page 657

show license udi with Standalone Product Instance

The following is sample output from the **show license udi** command on a standalone product instance.

```
Device# show license udi

UDI: PID:C9800-L-F-K9,SN:FCW2323W016
```

show license udi with Active and Standby

The following is sample output from the **show license udi** command in a High Availability set-up where an active and a standby product instances exist. UDI information is displayed for both.

```
Device# show license udi

UDI: PID:C9800-CL-K9,SN:93BBAH93MGS

HA UDI List:
    Active:PID:C9800-CL-K9,SN:93BBAH93MGS
    Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN
```

show license usage

To display license usage information such as status, a count of licenses being used, and enforcement type, enter the **show license usage** command in privileged EXEC mode.

show license usage

Syntax Description

This command has no keywords or arguments

Command Modes

Privileged EXEC

Command History

Release	Modification
This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy. This includes the `Status`, `Enforcement type` fields. Command output was also updated to remove reservation related information, authorization status information, and export status information.

Usage Guidelines

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Examples

See Table 15: show license usage Field Descriptions, on page 658 for information about fields shown in the display.

show license usage with unenforced licenses (Smart Licensing Using Policy), on page 659

show license usage with unenforced SLR licenses (Smart Licensing Using Policy), on page 660

Table 15: show license usage Field Descriptions

Field	Description
License Authorization: Status:	Displays overall authorization status.
():	Name of the license as in CSSM. If this license is one that requires an authorization code, the name of the license comes from the code.

Field	Description
Description	Description of the license as in CSSM.
Count	License count. If the license is not in-use, the count is reflected as zero.
Version	Version.
Status	License status can be one of the following • In-Use: Valid license, and in-use. • Not In-Use • Not Authorized: Means that the license requires installation of SLAC before use. For more information, see
Export Status:	Indicates if this license is export-controlled or not. Accordingly, one of the following statuses is displayed: • RESTRICTED - ALLOWED • RESTRICTED - NOT ALLOWED • NOT RESTRICTED
Feature name	Name of the feature that uses this license.
Feature Description:	Description of the feature that uses this license.
Utility Subscription id:	ID Not applicable, because the corresponding confiuration option is not supported.
Enforcement type	Enforcement type status for the license. This may be one of the following: • ENFORCED • NOT ENFORCED • EXPORT RESTRICTED - ALLOWED • EXPORT RESTRICTED - NOT ALLOWED For more information about enforcement types, see <link tbd>

show license usage with unenforced licenses (Smart Licensing Using Policy)

The following is sample output of the **show license usage** command. Unenforced licenses are in-use here.

```
Device# show license usage

License Authorization:
  Status: Not Applicable

air-network-essentials (DNA_NWSTACK_E):
  Description: air-network-essentials
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-network-essentials
  Feature Description: air-network-essentials
  Enforcement type: NOT ENFORCED
  License type: Perpetual

air-dna-essentials (AIR-DNA-E):
  Description: air-dna-essentials
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-dna-essentials
  Feature Description: air-dna-essentials
  Enforcement type: NOT ENFORCED
  License type: Perpetual
```

show license usage with unenforced SLR licenses (Smart Licensing Using Policy)

The following is sample output of the **show license usage** command. Migrated SLR licenses are in-use here:

```
Device# show license usage

air-network-advantage (DNA_NWStack):
  Description: air-network-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-network-advantage
  Feature Description: air-network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20

air-dna-advantage (AIR-DNA-A):
  Description: air-dna-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-dna-advantage
  Feature Description: air-dna-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20
```

show platform software sl-infra

To display troubleshooting information and for debugging, enter the **show platform software sl-infra** command in privileged EXEC mode. The output of this command is used by the technical support team, for troubleshooting and debugging.

show platform software sl-infra { **all** | **current** | **debug** | **stored** }

Syntax Description

all	Displays current, debugging, and stored information.
current	Displays current license-related information.
debug	Enables debugging
stored	Displays information that is stored on the product instance.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	This command was introduced.

Usage Guidelines

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra all** privileged EXEC commands.

show platform software tls client summary

To view the TLS client summary details, use the **show platform software tls client summary** command.

show platform software tls client summary

Syntax Description

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Examples

This example shows how to view the TLS client summary details:

```
Device # show platform software tls client summary

Name     ID     Gateway   Port   Auth     Trustpoint   DPD Time Rekey Time  Retry Time
-------------------------------------------------------------------------------------
fqdn     0               8443   PSK       N/A           60       300         20
```

show platform software client detail

To display a summary of TLS client session detail, session statistics, tunnel statistics, and DNS counters, use the **show platform software client detail** command.

show platform software client detail

Syntax Description

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Examples

This example shows how to view the TLS client summary details:

```
Device # show platform software client detail

TLS Client           : Session Detail
Session Name         : fqdn
FQDN resolved IP     : 10.194.234.149
ID                   : 0
Created              : 04/20/21 00:36:42
Updated              : 04/22/21 05:56:03
State                : Up (Rekey)
Up Time              : 04/21/21 20:30:21 ( 9 hours 25 minutes 45 seconds )
Down Time            : 04/21/21 20:30:01
Rekey Time           : 04/22/21 05:55:51 ( 15 seconds )

TLS Session Statistics

Up Notifications     : 3
Down Notifications   : 2
Rekey Notifications  : 636
DP State Updates     : 0
DPD Cleanups         : 0

Packets From     Packets To  Packet Errors To     Bytes From           Bytes To
-------------------------------------------------------------------------------
  BinOS              80           0                                      0
  IOSd                0           0                    0                 0

  TLS Client          0           0                    0                 0


TLS Tunnel Statistics
Type            Tx Packets      Rx Packets
-----------------------------------------
  Total              0               80
  CSTP Ctrl       3836             3836
  CSTP Data         80                0

Type            Requests         Responses
-----------------------------------------
```

```
CSTP Cfg          639                 639
CSTP DPD         3197                3197

Invalid CSTP Rx          : 0
Injected Packet Success  : 0
Injected Packet Failed   : 0
Consumed Packets         : 0

TLS Tunnel DNS Counters
DNS Resolve Request Success Count    : 641
DNS Resolve Request Failure Count    :  0
DNS Resolve Success Count            : 639
DNS Resolve Failure Count            :  2
```

show platform software tls statistics

To view the TLS client global statistic details, use the **show platform software tls statistics** command.

show platform software tls statistics

Syntax Description

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Examples

This example shows how to view the TLS client summary details:

```
Device # show platform software tls statistics

TLS Client - Global Statistics
Session Statistics
Up/Down           : 5/2
Rekeys            : 636
DP Updates        :   0
DPD Cleanups      :   0

Packets From    Packets To   Packet Errors To     Bytes From   Bytes To
-------------------------------------------------------------------------
BinOS              85             0                  0             0
IOSd 0             0              0                  0             0
TLS Client  0      0                                 0             0

Tunnel Statistics
SSL Handshake Init/Done     : 641/641
TCP Connection Req/Done     : 641/641

Tunnel Packets
Rx/Tx                       : 85/0
Injected / Failed           : 0/0
Consumed                    :  0

CSTP Packets
Control Rx/Tx               : 3839 / 3839
Data Rx/Tx                  : 0 / 85
Config Req/Resp             : 641 / 641
DPD Req/Resp                : 3198 / 3198
Invalid Rx                  : 0

FQDN Counters
Req/Resp/Success            : 0/0/0

NAT Counters
Transalte In/Out            : 0/0
Ignore    In/Out            : 0/0
Failed                      : 0
Invalid                     : 0
```

```
No Entry                    : 0
Unsupported                 : 0

Internal Counters
Type           Allocated            Freed
------------------------------------------------
EV              1299                 1295
Tunnel             5                    4
Conn             643                  642
Sess               3                    2

Config Message Related Counters
Type               Success              Failed
------------------------------------------------
Create                   3                   0
Delete                   2                   0
```

show platform software tls session summary

To view the tls client session summary, use the **show platform software tls session summary** command.

show platform software tls session summary

Syntax Description

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Examples

This example shows how to view the TLS client summary details:

```
Device # show platform software tls session summary

TLS Client - Session Summary
Name     ID      Created            State    Since               Elapsed
-------------------------------------------------------------------------------------------
fqdn     0      04/20/21 00:36:42    Up     04/21/21 20:30:21   9 hours 26 minutes 44 seconds
```

show logging profile wireless end timestamp

To specify log filtering end location timestamp for filtering, use the **show logging profile wireless end timestamp** command.

show logging profile wireless end timestamp *time-stamp*

Syntax Description

time-stamp	Time to end the filtering. For example, 2017/02/10 14:41:50.849.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Ensure that you enable internal keyword using the **show logging profile wireless internal** command to get the trace output.

Example

The following example shows how to specify log filtering end location timestamp for filtering:

```
Device# show logging profile wireless end timestamp 2017/02/10 14:41:50.849
```

show logging profile wireless filter

To specify filter for logs, use the **show logging profile wireless filter** command.

show logging profile wireless filter { **ipv4** | **mac** | **string** | **uuid** }

Syntax Description

ipv4	Selects logs with specific IP address app context.
mac	Selects logs with specific MAC app context.
string	Selects logs with specific string app context.
uuid	Selects logs with specific Universally Unique Identifier (UUID) app context.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

Example

The following example shows how to specify filter for logs:

```
Device# show logging profile wireless filter ipv4 10.10.11.1
```

show logging profile wireless fru

To specify field-replaceable unit (FRU) specific commands, use the **show logging profile wireless fru** command.

show logging profile wireless fru {0 {reverse | to-file}| chassis} {**0** {**reverse** | **to-file**} | **chassis**}

Syntax Description

0	SPA-Inter-Processor slot 0.
reverse	Shows logs in reverse chronological order.
to-file	Decodes files stored in disk and write output to file.
chassis	Chassis name.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

Example

The following example shows how to specify FRU specific commands:

```
Device# show logging profile wireless fru 0
```

show logging profile wireless internal

To select all the logs, use the **show logging profile wireless internal** command.

show logging profile wireless internal

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

Example

The following example shows how to display all the logs:

```
Device# show logging profile wireless internal
```

show logging profile wireless level

To select logs above a specific level, use the **show logging profile wireless level** command.

show logging profile wireless level { **debug** | **emergency** | **error** | **info** | **noise** | **notice** | **verbose** | **warning** }

Syntax Description

debug	Selects debug messages.
emergency	Selects emergency possible messags.
error	Selects error messages.
info	Selects informational messages.
noise	Selects maximum possible messages.
notice	Selects notice messages.
verbose	Selects verbose debug messages.
warning	Selects warning messages.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

Example

The following example shows how to select logs above a specific level:

```
Device# show logging profile wireless level info
```

show logging profile wireless module

To select logs for specific modules, use the **show logging profile wireless module** command.

show logging profile wireless module *module-name*

Syntax Description

module-name	A comma or space separated list of module names. For example, dbal, tdllib or "dbal tdllib".

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

Example

The following example shows how to select logs for specific modules:

```
Device# show logging profile wireless module dbal
```

show logging profile wireless reverse

To view logs in reverse chronological order, use the **show logging profile wireless reverse** command.

show logging profile wireless reverse

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

Example

The following example shows how to view logs in reverse chronological order:

```
Device# show logging profile wireless reverse
```

show logging profile wireless start

To specify log filtering start location, use the **show logging profile wireless start** command.

show logging profile wireless start {**marker** *marker* | **timestamp** *time-stamp*}

Syntax Description

marker	The marker to start filtering from. It must match with previously set marker.
timestamp	The timestamp for filtering. for example, "2017/02/10 14:41:50.849".

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

Example

The following example shows how to specify log filtering start location:

```
Device# show logging profile wireless start timestamp 2017/02/10 14:41:50.849
```

show logging profile wireless switch

To specify the switch to look for logs, use the **show logging profile wireless switch** command.

show logging profile wireless switch {*switch-num* | **active** | **standby**}

Syntax Description

active	Selects the active instance.
standby	Selects the standby instance.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

Example

The following example shows how to specify the number to look for logs:

```
Device# show logging profile wireless switch active
```

show logging profile wireless to-file

To decode files stored in disk and write the output to a file, use the **show logging profile wireless to-file** command.

show logging profile wireless to-file *output-file-name*

Syntax Description

output-file-name	Output file name. File with this name will be created in the flash memory.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

Example

The following example shows how to decode files stored in disk and write the output to a file:

```
Device# show logging profile wireless to-file testfile
```

show nmsp

To display the Network Mobility Services Protocol (NMSP) configuration settings, use the **show nmsp** command.

show nmsp {**attachment** | {**suppress interfaces**} | **capability** | **notification interval** | **statistics** {**connection** | **summary**} | **status** | **subscription detail** [*ip-addr*] | **summary**}

Syntax Description

attachment suppress interfaces	Displays attachment suppress interfaces.
capability	Displays NMSP capabilities.
notification interval	Displays the NMSP notification interval.
statistics connection	Displays all connection-specific counters.
statistics summary	Displays the NMSP counters.
status	Displays status of active NMSP connections.
subscription detail *ip-addr*	The details are only for the NMSP services subscribed to by a specific IP address.
subscription summary	Displays details for all of the NMSP services to which the controller is subscribed. The details are only for the NMSP services subscribed to by a specific IP address.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following is sample output from the **show nmsp notification interval** command:

```
Device#  show nmsp notification interval
NMSP Notification Intervals
---------------------------

RSSI Interval:
 Client               : 2 sec
 RFID                 : 2 sec
 Rogue AP             : 2 sec
 Rogue Client         : 2 sec
Attachment Interval   : 30 sec
Location Interval     : 30 sec
```

show nmsp cloud-services statistics

To see NMSP cloud-service statistics, use the **show nmsp cloud-services statistics** command.

show nmsp cloud-services statistics [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

chassis-number	Chassis number as either 1 or 2.
active R0	Active instance of the active NMSP cloud services in Route-processor slot 0.
standby R0	Standby instance of the active NMSP cloud services in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

This example shows how to see NMSP cloud-service statistics:

```
Device# show nmsp cloud-services statistics
```

show nmsp cloud-services summary

To see a summary of information about NMSP cloud-services, use the **show nmsp cloud-services summary** command.

show nmsp cloud-services summary [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

chassis-number	Chassis number as either 1 or 2.
active R0	Active instance of the NMSP cloud services in Route-processor slot 0.
standby R0	Standby instance of the active NMSP cloud services in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

This example shows how to see NMSP cloud-service summary information:

```
Device# show nmsp cloud-services summary
```

show nmsp subscription group detail all

To display the mobility services group subscription details of all CMX connections, use the **show nmsp subscription group detail all** command.

show nmsp subscription group detail all

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to display the mobility services group subscription details of all CMX connections:

```
Device# show nmsp subscription group detail all
```

show nmsp subscription group detail ap-list

To display the AP MAC list subscribed for a group by a CMX connection, use the **show nmsp subscription group detail ap-list** command.

show nmsp subscription group detail ap-list *group-name cmx-IP-addrress*

Syntax Description

group-name	CMX AP group name.
cmx-IP-addrress	CMX IP address.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to verify the AP MAC list subscribed for a group by a CMX connection.

```
Device# show nmsp subscription group detail ap-list Group1 127.0.0.1

CMX IP address: 127.0.0.1
CMX Group name: Group1
CMX Group AP MACs:
: 00:00:00:00:70:02  00:00:00:00:66:02  00:99:00:00:00:02  00:00:00:bb:00:02
  00:00:00:00:55:02  00:00:00:00:50:02  00:33:00:00:00:02  00:d0:00:00:00:02
  00:10:00:10:00:02  00:00:00:06:00:02  00:00:00:02:00:02  00:00:00:00:40:02
  00:00:00:99:00:02  00:00:00:00:a0:02  00:00:77:00:00:02  00:22:00:00:00:02
  00:00:00:00:00:92  00:00:00:00:00:82  00:00:00:00:03:02  aa:00:00:00:00:02
  00:00:00:50:00:42  00:00:0d:00:00:02  00:00:00:00:00:32  00:00:00:cc:00:02
  00:00:00:88:00:02  20:00:00:00:00:02  10:00:00:00:00:02  01:00:00:00:00:02
  00:00:00:00:00:02  00:00:00:00:00:01  00:00:00:00:00:00
```

show nmsp subscription group detail services

To display the services subscribed for a group by a CMX connection, use the **show nmsp subscription group detail services** command.

show nmsp subscription group detail services *group-name cmx-IP-addrress*

Syntax Description

group-name	CMX AP group name.
cmx-IP-addrress	CMX IP address.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to verify the services subscribed for a group by a CMX connection.

```
Device# show nmsp subscription group detail services Group1 127.0.0.1

CMX IP address: 127.0.0.1
CMX Group name: Group1
CMX Group filtered services:
Service            Subservice
----------------------------
RSSI               Mobile Station,
Spectrum
Info
Statistics
```

show nmsp subscription group summary

To display the mobility services group subscription summary of all CMX connections, use the **show nmsp subscription group summary** command.

show nmsp subscription group summary

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to verify the mobility services group subscription summary of all CMX connections.

```
Device# show nmsp subscription group summary

CMX IP address: 127.0.0.1
  Groups subscribed by this CMX server:
  Group name: Group1
```

show platform conditions

To see information about conditional debugs, use the **show platform conditions** command.

show platform conditions

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see information about conditional debugs:

```
Device# show platform conditions
```

show platform software wlavc status cp-exporter

To view the wireless AVC information from the control place exporter, use the **show platform software wlavc status cp-exporter** command.

show platform software wlavc status cp-exporter

Syntax Description

wlavc	Displays the wireless AVC information.
status	Displays information about the AVC status.
cp-exporter	Collects information from the Control Plane exporter.

Command Default

None

Command Modes

Privileged EXEC (#) mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

Example

This example shows how to display the wireless AVC information from the control place exporter:

```
show platform software wlavc status cp-exporter
AVC FNF Exporter status
IP: 10.10.1.1
connection statistics
Sent bytes : 5672
Sent packets : 569
Received records : 564
Socket statistics
New sockets : 3
Closed sockets : 0
Library statistics AVC
cache errors : 0
Unexpected Flow Monitor ID : 0
Socket creation error : 0
Sent records : 240
Received packets : 800
```

show platform software system all

To check status of the current virtual machine and look for performance issues due to inadequate resources (or other issues with the hosting environment), use the **set platform software system all** command in privileged EXEC mode.

show platform software system all

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

This example shows how to check status of the current virtual machine and its resources:

```
Device# show platform software system all

Processor Details
=================
Number of Processors : 6
Processor : 1 - 6
vendor_id : GenuineIntel
cpu MHz  : 2593.750
cache size : 35840 KB
Crypto Supported : Yes
model name : Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz

Memory Details
==============
Physical Memory : 16363904KB

VNIC Details
============
Name   Mac Address  Status Platform MTU
GigabitEthernet1 000c.2964.7126  UP 1500
GigabitEthernet2 000c.2964.7130  UP 1500

Hypervisor Details
==================
Hypervisor: VMWARE
Manufacturer: VMware, Inc.
Product Name: VMware Virtual Platform
Serial Number: VMware-56 4d e5 0a a7 dd 27 2b-0e 2f 36 6e 0f 64 71 26
UUID: 564DE50A-A7DD-272B-0E2F-366E0F647126
image_variant :

Boot Details
==================
Boot mode: BIOS
Bootloader version: 1.1
```

show platform software trace filter-binary

To display the most recent trace information for a specific module, use the **show platform software trace filter-binary** command in privileged EXEC or user EXEC mode.

show platform software trace filter-binary*modules* [**context** *mac-address*]

Syntax Description

context*mac-address*	Represents the context used to filter. Additionally, you can filter based on module names and trace levels. The context keyword accepts either a MAC address or any other argument based on which a trace is tagged.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

This command collates and sorts all the logs present in the `/tmp/.../` across all the processes relevant to the module. The trace logs of all the processes relevant to the specified module are printed to the console. This command also generates a file named `collated_log_{system time}` with the same content, in the `/crashinfo/tracelogs` directory.

Examples

This example shows how to display the trace information for a wireless module:

```
Device# show platform software trace filter-binary wireless
```

show platform software trace level

To view the trace levels for all the modules under a specific process, use the **show platform software trace level** command in privileged EXEC or user EXEC mode.

Syntax Description

process	Process whose tracing level is being set. Options include: • **chassis-manager**—The Chassis Manager process. • **cli-agent**—The CLI Agent process. • **cmm**—The CMM process. • **dbm**—The Database Manager process. • **emd**—The Environmental Monitoring process. • **fed**—The Forwarding Engine Driver process. • **forwarding-manager**—The Forwarding Manager process. • **geo**—The Geo Manager process. • **host-manager**—The Host Manager process. • **interface-manager**—The Interface Manager process. • **iomd**—The Input/Output Module daemon (IOMd) process. • **ios**—The IOS process. • **license-manager**—The License Manager process. • **logger**—The Logging Manager process. • **platform-mgr**—The Platform Manager process. • **pluggable-services**—The Pluggable Services process. • **replication-mgr**—The Replication Manager process. • **shell-manager**—The Shell Manager process. • **sif**—The Stack Interface (SIF) Manager process. • **smd**—The Session Manager process. • **stack-mgr**—The Stack Manager process. • **table-manager**—The Table Manager Server. • **thread-test**—The Multithread Manager process. • **virt-manager**—The Virtualization Manager process. • **wireless**—The wireless controller module process.

slot	Hardware slot where the process for which the trace level is set, is running. Options include:
	• *number*—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2.
	• *SIP-slot / SPA-bay*—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2.
	• **F0**—The Embedded Service Processor in slot 0.
	• **F1**—The Embedded Service Processor in slot 1.
	• **FP active**—The active Embedded Service Processor.
	• **R0**—The route processor in slot 0.
	• **RP active**—The active route processor.
	• **switch** <*number*> —The switch, with its number specified.
	• **switch active**—The active switch.
	• **switch standby**—The standby switch.
	  • *number*—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2.
	  • *SIP-slot / SPA-bay*—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2.
	  • **F0**—The Embedded Service Processor in slot 0.
	  • **FP active**—The active Embedded Service Processor.
	  • **R0**—The route processor in slot 0.
	  • **RP active**—The active route processor.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Examples

This example shows how to view the trace level:

```
Device#  show platform software trace level dbm chassis active R0
```

```
Module Name                      Trace Level
----------------------------------------------------
binos                            Notice
binos/brand                      Notice
bipc                             Notice
btrace                           Notice
bump_ptr_alloc                   Notice
cdllib                           Notice
chasfs                           Notice
dbal                             Informational
dbm                              Debug
evlib                            Notice
evutil                           Notice
file_alloc                       Notice
green-be                         Notice
ios-avl                          Notice
klib                             Debug
services                         Notice
sw_wdog                          Notice
syshw                            Notice
tdl_cdlcore_message              Notice
tdl_dbal_root_message            Notice
tdl_dbal_root_type               Notice
```

show platform software trace message

To display the trace messages for a process, use the **set platform software trace** command in privileged EXEC or user EXEC mode.

show platform software trace message *process* **chassis** { *<1-2>* | **active** | **standby** } **R0**

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Examples

This example shows how to display the trace messages for the Stack Manager and the Forwarding Engine Driver processes:

```
Device# show platform software trace message stack-mgr switch active R0
10/30 09:42:48.767 [btrace] [8974]: (note): Successfully registered module [97] [uiutil]
10/30 09:42:48.762 [btrace] [8974]: (note): Successfully registered module [98]
[tdl_cdlcore_message]
10/29 13:28:19.023 [stack_mgr] [8974]: (note): Examining peer state
10/29 13:28:19.023 [stack_mgr] [8974]: (note): no switch eligible for standby election
presently
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Posting event
stack_fsm_event_wait_standby_elect_timer_expired, curstate stack_fsm_state_active_ready
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Timer HDL - STACK_WAIT_STANDBY_ELECT_TIMER
expired
10/29 13:26:46.584 [btrace] [8974]: (note): Successfully registered module [99]
[tdl_ui_message]
10/29 13:26:46.582 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:36.582 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect
10/29 13:26:36.582 [evutil] [8974]: (ERR): Asynchronous connect failed for [uipeer uplink
to slot 1] (fd == -1)
10/29 13:26:36.581 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:26.581 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect
```

show platform software trace message license-manager chassis active R0

To display the trace message for license-manager process of active route processor, use the **show platform software trace message license-manager chassis active R0** command in privileged EXEC mode.

```
show platform software trace message license-managerchassis {chassis-number
| active | standby}R0reverse
```

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to display the trace messages for the Forwarding Engine Driver processes:

```
Device# show platform software trace message license-manager chassis active R0
.......
2018/06/25 07:16:53.121 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Decode of the file /tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy completed in 35
 msecs
/tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy: DECODE(50:50:0:7)
2018/06/25 07:16:53.088 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Decode of file [/tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy] returned [0]
2018/06/25 06:53:20.421 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Decode of the file /tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy completed in 34
 msecs
2018/06/25 06:53:20.389 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Decode of file [/tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy] returned [0]
2018/06/20 07:55:10.540 {lman_R0-0}{1}: [trccfg] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Processing all-modules
2018/06/20 07:55:10.540 {lman_R0-0}{1}: [trccfg] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Empty trace conf file
2018/06/20 07:54:46.453 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Constructing domain iosd_lmrp for RP/0/0 to RP/0/0
2018/06/20 07:54:46.453 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Received registration msg from [IOS]
2018/06/20 07:54:46.449 {lman_R0-0}{1}: [bipc] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Received a connection from client for path /tmp/rp/lipc/license_mgr_socket
2018/06/20 07:54:45.557 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:44.556 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:43.556 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:42.555 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:41.554 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
```

```
2018/06/20 07:54:40.553 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:39.553 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:38.552 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:37.551 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:36.550 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:35.550 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:34.549 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:33.548 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:32.547 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:31.547 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:30.547 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:30.537 {lman_R0-0}{1}: [bipc] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Pending connection to server 10.0.1.0
2018/06/20 07:54:29.546 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:28.545 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:27.545 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:26.544 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:25.543 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:24.542 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:23.542 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:22.541 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:21.540 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:20.633 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note): Peer
 attach: from location R0:0 is successful
2018/06/20 07:54:20.633 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note): Not
 setting domain for cmand
2018/06/20 07:54:20.625 {lman_R0-0}{1}: [bipc] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Received a connection from client for path /tmp/rp/lipc/lman_lic_serv_socket
2018/06/20 07:54:20.624 {lman_R0-0}{1}: [tdllib] [21231]: UUID: 0, ra: 0, TID: 0 (note):
epoch file read /tmp/tdlresolve/epoch_dir//2018_06_20_07_54_2413.epoch
2018/06/20 07:54:20.624 {lman_R0-0}{1}: [tdllib] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Detect newly epoch file generated: new epoch:
/tmp/tdlresolve/epoch_dir//2018_06_20_07_54_2413.epoch
2018/06/20 07:54:20.624 {lman_R0-0}{1}: [tdllib] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Flag tdlh stale epoch for all tdl handles
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Chasfs Watch on rp/0/0/rtu_licensing for platform to create RTU properties
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note): The
 chassis product id: 'ISR4461/K9'
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note): The
 chassis serial number: 'FDO2213A0GL'
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [bcrdu] [21231]: UUID: 0, ra: 0, TID: 0 (note):
CRDU
/tmp/sw/mount/isr4400v2-mono-universalk9.BLD_V169_THROTTLE_LATEST_20180618_044856_V16_9_0_163.SSA.pkg/usr/binos/bin/lman
```

```
 proc path is /tmp/patch/CRDU/BPROC_LM_RP/
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [bcrdu] [21231]: UUID: 0, ra: 0, TID: 0 (note):
CRDU
/tmp/sw/mount/isr4400v2-mono-universalk9.BLD_V169_THROTTLE_LATEST_20180618_044856_V16_9_0_163.SSA.pkg/usr/binos/bin/lman
 procstr is BPROC_LM_RP
2018/06/20 07:54:20.533 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note): No
licensing objects present in chasfs to delete
2018/06/20 07:54:20.533 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Deleting any existing licensing chasfs objects under [rp/0/0/licensing]
2018/06/20 07:54:20.532 {lman_R0-0}{1}: [syshw] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): syshw
 build device: could not add register 7 dev:
/sys/bus/platform/devices/cpld/reg_rp_sku_register (No such file or directory) due to No
such file or directory
2018/06/20 07:54:20.532 {lman_R0-0}{1}: [syshw] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): syshw
 build device: could not add register 5 dev: /sys/bus/platform/devices/cpld/phys_slot_number
 (No such file or directory) due to No such file or directory

Total messages : 49
```

show policy-map

To display quality of service (QoS) policy maps, which define classification criteria for incoming traffic, use the **show policy-map** command in EXEC mode.

show policy-map [{*policy-map-name* | **interface** *interface-id*}]

show policy-map interface {**Auto-template** | **Capwap** | **GigabitEthernet** | **GroupVI** | **InternalInterface** | **Loopback** | **Lspvif** | **Null** | **Port-channel** | **TenGigabitEthernet** | **Tunnel** | **Vlan** | **brief** | **class** | **input** | **output**

show policy-map interface {**ap name** *ap_name* | **client mac** *mac_address* | **radio type** {**24ghz** | **5ghz**} **ap name** *ap_name* | **ssid name** *ssid_name* {**ap name** *ap_name* | **radio type** {**24ghz** | **5ghz**} **ap name** *ap_name*} }

Syntax Description

policy-map-name	(Optional) Name of the policy-map.
interface *interface-id*	(Optional) Displays the statistics and the configurations of the input and output policies that are attached to the interface.
ap name *ap_name*	Displays SSID policy configuration of an access point.
client mac *mac_address*	Displays information about the policies for all the client targets.
radio type {**24ghz** | **5ghz**	Displays policy configuration of the access point in the specified radio type.
ssid name *ssid_name*	Displays policy configuration of an SSID.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.

Note Though visible in the command-line help string, the **control-plane**, **session**, and **type** keywords are not supported, and the statistics shown in the display should be ignored.

To display classification counters for ternary content addressable memory (TCAM) (marking or policing) based policies, enter the interface ID. Classification counters have the following restrictions:

- Classification counters are supported only on wired ports (in the ingress and egress directions).
- Classification counters count packets instead of bytes.
- Only QoS configurations with marking or policing trigger the classification counter.
- As long as there is policing or marking action in the policy, the class-default will have classification counters.
- Classification counters are not port based. The counters are shared across targets sharing the same policy map. This means that the classification counter aggregates all packets belonging to the same class of the same policy which attach to different interfaces.

This is an example of output from the **show policy-map interface** command, where classification counters are displayed:

```
Device# show policy-map interface gigabitethernet1/0/1

  GigabitEthernet1/0/1

  Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy

    Class-map: AutoQos-4.0-Voip-Data-CiscoPhone-Class (match-any)
      0 packets
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp ef
      police:
          cir 128000 bps, bc 8000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          set-dscp-transmit dscp table policed-dscp
        conformed 0000 bps, exceed 0000 bps

    Class-map: AutoQos-4.0-Voip-Signal-CiscoPhone-Class (match-any)
      0 packets
      Match: cos  3
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp cs3
      police:
          cir 32000 bps, bc 8000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          set-dscp-transmit dscp table policed-dscp
        conformed 0000 bps, exceed 0000 bps
```

```
  Class-map: AutoQos-4.0-Default-Class (match-any)
    0 packets
    Match: access-group name AutoQos-4.0-Acl-Default
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp default

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
    Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
    queue-limit dscp 16 percent 80
    queue-limit dscp 24 percent 90
    queue-limit dscp 48 percent 100
    queue-limit dscp 56 percent 100

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%

    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
    0 packets
    Match:  dscp af41 (34) af42 (36) af43 (38)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  4
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
```

```
  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
```

```
  5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25
```

show ssh

To see the SSH connection status, use the **show ssh** command.

show ssh {*connection-number* | {**vty** *connection-number* }}

Syntax Description

connection-number	SSH connection number. Valid range is 0 to 530.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the SSH connection status:

```
Device# show ssh connection-number
```

show tech-support wireless

To display Cisco wireless LAN controller variables frequently requested by Cisco Technical Assistance Center (TAC), use the **show tech-support wireless** command in privileged EXEC mode.

show tech-support wireless

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following is sample output from the **show tech-support wireless** command:

```
Device# show tech-support wireless
 *** show ap capwap timers ***

Cisco AP CAPWAP timers

AP Discovery timer       : 10
AP Heart Beat timeout    : 30
Primary Discovery timer  : 120
Primed Join timeout      : 0
Fast Heartbeat           : Disabled
Fast Heartbeat timeout   : 1
*** show ap capwap retransmit ***
Global control packet retransmit interval : 3
Global control packet retransmit count : 5

AP Name                           Retransmit Interval             Retransmit Count
-----------------------------------------------------------------------------------------
TSIM_AP-2                         3                               5
TSIM_AP-3                         3                               5
*** show ap dot11 24ghz cleanair air-quality summary ***

AQ = Air Quality
DFS = Dynamic Frequency Selection

*** show ap dot11 24ghz cleanair air-quality worst ***

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name             Channel   Avg AQ  Min AQ  Interferers  DFS
-----------------------------------------------------------------
                    0         0       0       0            No
*** show ap dot11 24ghz cleanair config ***

Clean Air Solution................................ : Disabled
Air Quality Settings:
    Air Quality Reporting......................... : Disabled
    Air Quality Reporting Period (min)............ : 15
```

```
    Air Quality Alarms..................... : Enabled
    Air Quality Alarm Threshold............ : 10
Interference Device Settings:
    Interference Device Reporting.......... : Enabled
        Bluetooth Link..................... : Enabled
        Microwave Oven..................... : Enabled
        802.11 FH.......................... : Enabled
        Bluetooth Discovery................ : Enabled
        TDD Transmitter.................... : Enabled
        Jammer............................. : Enabled
        Continuous Transmitter............. : Enabled
        DECT-like Phone.................... : Enabled
        Video Camera....................... : Enabled
        802.15.4........................... : Enabled
        WiFi Inverted...................... : Enabled
        WiFi Invalid Channel............... : Enabled
        SuperAG............................ : Enabled
        Canopy............................. : Enabled
        Microsoft Device................... : Enabled
        WiMax Mobile....................... : Enabled
        WiMax Fixed........................ : Enabled
    Interference Device Types Triggering Alarms:
        Bluetooth Link..................... : Disabled
        Microwave Oven..................... : Disabled
        802.11 FH.......................... : Disabled
        Bluetooth Discovery................ : Disabled
        TDD Transmitter.................... : Disabled
        Jammer............................. : Disabled
        Continuous Transmitter............. : Disabled
        DECT-like Phone.................... : Disabled
        Video Camera....................... : Disabled
  802.15.4............................... : Disabled
        WiFi Inverted...................... : Enabled
        WiFi Invalid Channel............... : Enabled
        SuperAG............................ : Disabled
        Canopy............................. : Disabled
        Microsoft Device................... : Disabled
        WiMax Mobile....................... : Disabled
        WiMax Fixed........................ : Disabled
    Interference Device Alarms............. : Enabled
Additional Clean Air Settings:
    CleanAir Event-driven RRM State........ : Disabled
    CleanAir Driven RRM Sensitivity........ : LOW
    CleanAir Persistent Devices state...... : Disabled
```

show tech-support wireless ap

To display specific information about the Cisco APs variables frequently requested by Cisco Technical Assistance Center (TAC), use the **show tech-support wireless ap** command in privileged EXEC mode.

show tech-support wireless ap

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The output of the following commands are displayed as part of **show tech-support wireless ap**command:

- show ap session termination statistics
- show ap status
- show ap tag summary
- show platform software bssid chassis active F0 statistics
- show platform software bssid chassis active R0 statistics
- show platform software capwap chassis active F0 statistics
- show platform software capwap chassis active R0 statistics
- show platform software dtls chassis active F0 statistics
- show platform software dtls chassis active R0 statistics
- show platform software radio chassis active F0 statistics
- show platform software radio chassis active R0 statistics

Example

The following is sample output from the **show tech-support wireless ap** command

```
Device# show tech-support wireless ap

------------------ show platform software dtls chassis active R0 statistics ------------------


DTLS Counters     (Success/Failure)
-----------------------------------
Create                  0/0
```

```
Delete                  0/0

Switch 1:
OM Create               0/0
OM Delete               0/0
Ack Nack Notify         0/0


------------------ show platform software radio chassis active R0 statistics
------------------



Switch 1:
NACK Notify             0/0
  Create Failure        0
  Delete Failure        0


------------------ show platform software bssid chassis active R0 statistics
------------------



Switch 1:
NACK Notify             0/0
  Create Failure        0
  Delete Failure        0


------------------ show platform software capwap chassis active R0 statistics
------------------


Capwap Counters   (Success/Failure)
-----------------------------------
Create                  0/0
Delete                  0/0
Modify                  0/0

Switch 1:
OM Create               0/0
OM Delete               0/0
ACK-NACK Notify         0/0
  Tunnel State          0/0
  Tunnel Create         0/0
  Tunnel Modify         0/0
  Tunnel Delete         0/0


------------------ show platform software dtls chassis active F0 statistics ------------------


DTLS Counters     (Success/Failure)
-----------------------------------
Create                  0/0
Delete                  0/0
HW Create               0/0
HW Modify               0/0
HW Delete               0/0
Create Ack              0/0
Modify Ack              0/0
Delete Ack              0/0
Ack Ack Notify          0/0
```

```
Ack Nack Notify         0/0
Nack Notify             0/0
HA Seq GET              665/0
HA Seq SET              0/0
HA Seq Crypto GET       0/0
HA Seq Crypto SET       0/0
HA Seq Crypto Callback  0/0

HA Seq last Responsed   0
HA Seq Pending          0
HA Seq Outstanding cb   0


------------------ show platform software radio chassis active F0 statistics
------------------


Radio Counters    (Success/Failure)
-----------------------------------
Create                  0/0
Delete                  0/0
HW Create               0/0
HW Modify               0/0
HW Delete               0/0
Create Ack              0/0
Modify Ack              0/0
Delete Ack              0/0
Nack Notify             0/0


------------------ show platform software bssid chassis active F0 statistics
------------------


Bssid Counters    (Success/Failure)
-----------------------------------
Create                 0/0
Delete                 0/0
HW Create              0/0
HW Modify              0/0
HW Delete              0/0
Create Ack             0/0
Modify Ack             0/0
Delete Ack             0/0
Nack Notify            0/0


------------------ show platform software capwap chassis active F0 statistics
------------------


Capwap Counters   (Success/Failure)
-----------------------------------
Create                  0/0
Delete                  0/0
HW Create               0/0
HW Modify               0/0
HW Delete               0/0
Create Ack              0/0
Modify Ack              0/0
Delete Ack              0/0
Ack Ack Notify          0/0
Ack Nack Notify         0/0
Nack Notify             0/0
```

```
------------------ show ap auto-rf dot11 24ghz ------------------


------------------ show ap auto-rf dot11 5ghz ------------------


------------------ show ap capwap retransmit ------------------


------------------ show ap config dot11 dual-band summary ------------------


------------------ show ap config general ------------------



------------------ show ap dot11 24ghz channel ------------------


Leader Automatic Channel Assignment
  Channel Assignment Mode                   : AUTO
  Channel Update Interval                   : 600 seconds
  Anchor time (Hour of the day)             : 0
  Channel Update Contribution
    Noise                                   : Enable
    Interference                            : Enable
    Load                                    : Disable
    Device Aware                            : Disable
  CleanAir Event-driven RRM option          : Disabled
  Channel Assignment Leader                 : ewlc-doc (9.12.32.10)
  Last Run                                  : 25 seconds ago

  DCA Sensitivity Level                     : MEDIUM : 10 dB
  DCA Minimum Energy Limit                  : -95 dBm
  Channel Energy Levels
    Minimum                                 : unknown
    Average                                 : unknown
    Maximum                                 : -128 dBm
  Channel Dwell Times
    Minimum                                 : unknown
    Average                                 : unknown


------------------ show ap dot11 24ghz group ------------------


Radio RF Grouping

  802.11b Group Mode               : AUTO
  802.11b Group Update Interval    : 600 seconds
  802.11b Group Leader             : ewlc-doc (9.12.32.10)
  802.11b Last Run                 : 26 seconds ago


RF Group Members

Controller name                  Controller IP
```

```
-------------------------------------------------
ewlc-doc                          9.12.32.10



------------------ show ap dot11 24ghz load-info ------------------


------------------ show ap dot11 24ghz monitor ------------------


Default 802.11b AP monitoring
  802.11b Monitor Mode                : Enabled
  802.11b Monitor Channels            : Country channels
  802.11b RRM Neighbor Discover Type  : Transparent
  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
  802.11b NDP RSSI Normalization      : Enabled


------------------ 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
  802.11b 11M                             : Mandatory
  802.11g 6M                              : Supported
  802.11g 9M                              : Supported
  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


------------------ show ap dot11 24ghz profile ------------------


Default 802.11b AP performance profiles
  802.11b Global Interference threshold    : 10 %
  802.11b Global noise threshold           : -70 dBm
  802.11b Global RF utilization threshold  : 80 %
  802.11b Global throughput threshold      : 1000000 bps
  802.11b Global clients threshold         : 12 clients


------------------ show ap dot11 24ghz summary ------------------
```

```
------------------ show ap dot11 24ghz txpower ------------------


Automatic Transmit Power Assignment

Transmit Power Assignment Mode          : AUTO
Transmit Power Update Interval          : 600 seconds
Transmit Power Threshold                : -70 dBm
Transmit Power Neighbor Count           : 3 APs
Min Transmit Power                      : -10 dBm
Max Transmit Power                      : 30 dBm
Update Contribution
    Noise                               : Enable
    Interference                        : Enable
    Load                                : Disable
    Device Aware                        : Disable
Transmit Power Assignment Leader        : ewlc-doc (9.12.32.10)
Last Run                                : 27 seconds ago


------------------ show ap dot11 5ghz channel ------------------


Leader Automatic Channel Assignment
  Channel Assignment Mode                   : AUTO
  Channel Update Interval                   : 600 seconds
  Anchor time (Hour of the day)             : 0
  Channel Update Contribution
    Noise                                   : Enable
    Interference                            : Enable
    Load                                    : Disable
    Device Aware                            : Disable
  CleanAir Event-driven RRM option          : Disabled
  Channel Assignment Leader                 : ewlc-doc (9.12.32.10)
  Last Run                                  : 27 seconds ago

  DCA Sensitivity Level                     : MEDIUM : 15 dB
  DCA 802.11n/ac Channel Width              : 20 MHz
  DCA Minimum Energy Limit                  : -95 dBm
  Channel Energy Levels
    Minimum                                 : unknown
    Average                                 : unknown
    Maximum                                 : -128 dBm
  Channel Dwell Times
    Minimum                                 : unknown


------------------ show ap dot11 5ghz group ------------------


Radio RF Grouping

  802.11a Group Mode              : AUTO
  802.11a Group Update Interval   : 600 seconds
  802.11a Group Leader            : ewlc-doc (9.12.32.10)
  802.11a Last Run                : 28 seconds ago


RF Group Members

Controller name                  Controller IP
```

```
-------------------------------------------------
ewlc-doc                          9.12.32.10



------------------ show ap dot11 5ghz load-info ------------------


------------------ show ap dot11 5ghz monitor ------------------


Default 802.11a AP monitoring
  802.11a Monitor Mode                : Enabled
  802.11a Monitor Channels            : Country channels
  802.11a RRM Neighbor Discover Type  : Transparent
  802.11a AP Coverage Interval        : 180 seconds
  802.11a AP Load Interval            : 60 seconds
  802.11a AP Noise Interval           : 180 seconds
  802.11a AP Signal Strength Interval : 60 seconds
  802.11a NDP RSSI Normalization      : Enabled


------------------ 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


------------------ show ap dot11 5ghz profile ------------------


Default 802.11a AP performance profiles

  802.11a Global Interference threshold         : 10 %
  802.11a Global noise threshold                : -70 dBm
  802.11a Global RF utilization threshold       : 80 %
  802.11a Global throughput threshold           : 1000000 bps
  802.11a Global clients threshold              : 12 clients


------------------ show ap dot11 5ghz summary ------------------
```

```
------------------ show ap dot11 5ghz txpower ------------------


Automatic Transmit Power Assignment

Transmit Power Assignment Mode          : AUTO
Transmit Power Update Interval          : 600 seconds
Transmit Power Threshold                : -70 dBm
Transmit Power Neighbor Count           : 3 APs
Min Transmit Power                      : -10 dBm
Max Transmit Power                      : 30 dBm
Update Contribution
    Noise                               : Enable
    Interference                        : Enable
    Load                                : Disable
    Device Aware                        : Disable
Transmit Power Assignment Leader        : ewlc-doc (9.12.32.10)
Last Run                                : 28 seconds ago


------------------ show ap image ------------------



------------------ show wireless stats ap join summary ------------------

Number of APs: 0

Base MAC        Ethernet MAC    AP Name                           IP Address       Status
     Last Failure Type     Last Disconnect Reason
-----------------------------------------------------------------------------------------


------------------ show ap rf-profile summary ------------------


Number of RF-profiles: 6

RF Profile Name                  Band     Description                          State
------------------------------------------------------------------------------------
Low_Client_Density_rf_5gh        5 GHz    pre configured Low Client Density rf Up
High_Client_Density_rf_5gh       5 GHz    pre configured High Client Density r Up
Low_Client_Density_rf_24gh       2.4 GHz  pre configured Low Client Density rf Up
High_Client_Density_rf_24gh      2.4 GHz  pre configured High Client Density r Up
Typical_Client_Density_rf_5gh    5 GHz    pre configured Typical Density rfpro Up
Typical_Client_Density_rf_24gh   2.4 GHz  pre configured Typical Client Densit Up


------------------ show ap slots ------------------


------------------ show ap summary ------------------


Number of APs: 0
```

```
------------------ show ap uptime ------------------

Number of APs: 0


------------------ show ap tag summary ------------------

Number of APs: 0


------------------ show ap status ------------------


------------------ show ap cdp neighbors ------------------

Number of neighbors: 0


------------------ show ap ap-join-profile summary ------------------


Number of AP Profiles: 1
AP Profile Name                  Description
------------------------------------------------------------------------
default-ap-profile               default ap profile

------------------ show ap link-encryption ------------------


------------------ show wireless stats ap session termination ------------------


------------------ show wireless loadbalance ap affinity wncd 0 ------------------


------------------ show wireless loadbalance ap affinity wncd 1 ------------------


------------------ show wireless loadbalance ap affinity wncd 2 ------------------


------------------ show wireless loadbalance ap affinity wncd 3 ------------------


------------------ show wireless loadbalance ap affinity wncd 4 ------------------


------------------ show wireless loadbalance ap affinity wncd 5 ------------------
```

```
------------------- show wireless loadbalance ap affinity wncd 6 -------------------

------------------- show wireless loadbalance ap affinity wncd 7 -------------------
```

show tech-support wireless client

To print the data related to all clients or a particular client, use the **show tech-support wireless client** command in privileged EXEC mode.

show tech-support wireless client

Syntax Description

mac-address	Client MAC address.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The output of the following commands are displayed as part of **show tech-support wireless client** command:

- show platform software wireless-client chassis active F0 statistics
- show platform software wireless-client chassis active R0 statistics
- show wireless client calls active
- show wireless client calls rejected
- show wireless client client-statistics summary
- show wireless client device summary
- show wireless client mac <mac-addr> details
- show wireless client probing
- show wireless client sleeping-client
- show wireless client statistic
- show wireless client steering
- show wireless client summary
- show wireless exclusionlist
- show wireless pmk-cache

Example

The following is sample output from the **show tech-support wireless client** command

```
Device# show tech-support wireless client

------------------ show wireless stats client summary ------------------

Number of Local Clients : 0


MAC Address    AP Name                          WLAN UpTime(secs) Rx Pkts Tx Pkts RSSI SNR
  Data Retries
------------------------------------------------------------------------------------------




------------------ show wireless client summary ------------------

Number of Local Clients: 0


Number of Excluded Clients: 0



------------------ show wireless client device summary ------------------



------------------ show wireless client steering ------------------


Client Steering Configuration Information
  Macro to micro transition threshold                 : -55 dBm
  Micro to Macro transition threshold                 : -65 dBm
  Micro-Macro transition minimum client count         : 3
  Micro-Macro transition client balancing window      : 3
  Probe suppression mode                              : Disabled
  Probe suppression validity window                   : 100 s
  Probe suppression aggregate window                  : 200 ms
  Probe suppression transition aggressiveness         : 3
  Probe suppression hysteresis                        : -6 dBm

WLAN Configuration Information



------------------ show wireless client calls active ------------------



------------------ show wireless client calls rejected ------------------



------------------ show wireless client sleeping-client ------------------

Total number of sleeping-client entries: 0


------------------ show wireless client probing ------------------



------------------ show wireless client ap dot11 24ghz ------------------
```

```
------------------ show wireless client ap dot11 5ghz ------------------



------------------ show wireless pmk-cache ------------------

Number of PMK caches in total : 0

Type      Station             Entry Lifetime  VLAN Override         IP Override
Audit-Session-Id
-----------------------------------------------------------------------------------------------------


------------------ show wireless exclusionlist ------------------


------------------ show wireless country  configured ------------------


Configured Country.........................   US - United States
Configured Country Codes
        US  - United States                 802.11a Indoor/ 802.11b Indoor/ 802.11g Indoor


------------------ show wireless tag rf summary ------------------


Number of RF Tags: 1

RF tag name                        Description
------------------------------------------------------------------------
default-rf-tag                     default RF tag


------------------ show platform software wireless-client chassis active R0 statistics
------------------

Client Counters   (Success/Failure)
-----------------------------------
Create                  0/0
Delete                  0/0
Modify                  0/0

Switch 1:
OM Create               0/0
OM Delete               0/0
NACK Notify             0/0
  Create Failure        0
  Modify Failure        0
  Delete Failure        0
```

```
------------------ show platform software wireless-client chassis active F0 statistics
------------------


Client Counters   (Success/Failure)
-----------------------------------
Create                  0/0
Delete                  0/0
HW Create               0/0
HW Modify               0/0
HW Delete               0/0
Create Ack              0/0
Modify Ack              0/0
Delete Ack              0/0
NACK Notify             0/0
```

show tech-support wireless radio

To print the data related to the radio, use the **show tech-support wireless radio** command in privileged EXEC mode.

show tech-support wireless radio

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The output of the following commands are displayed as part of **show tech-support wireless radio** command:

- show ap auto-rf dot11 24ghz
- show ap auto-rf dot11 5ghz
- show ap config dot11 dual-band summary
- show ap config general
- show ap dot11 24ghz channel
- show ap dot11 24ghz coverage
- show ap dot11 24ghz group
- show ap dot11 24ghz high-density
- show ap dot11 24ghz load-info
- show ap dot11 24ghz monitor
- show ap dot11 24ghz network
- show ap dot11 24ghz summary
- show ap dot11 24ghz txpower
- show ap dot11 5ghz channel
- show ap dot11 5ghz coverage
- show ap dot11 5ghz group
- show ap dot11 5ghz high-density
- show ap dot11 5ghz load-info

- show ap dot11 5ghz monitor
- show ap dot11 5ghz network
- show ap dot11 5ghz summary
- show ap dot11 5ghz txpower
- show ap fra
- show ap rf-profile name Rf1 detail
- show ap rf-profile summary
- show ap summary
- show wireless band-select

Example

The following is sample output from the **show tech-support wireless radio** command

```
Device# show tech-support wireless radio

------------------ show ap summary ------------------

Number of APs: 0


------------------ show ap dot11 24ghz summary ------------------


------------------ show ap dot11 5ghz summary ------------------


------------------ show ap config dot11 dual-band summary ------------------


------------------ show ap dot11 24ghz channel ------------------


Leader Automatic Channel Assignment
  Channel Assignment Mode                   : AUTO
  Channel Update Interval                   : 600 seconds
  Anchor time (Hour of the day)             : 0
  Channel Update Contribution
    Noise                                   : Enable
    Interference                            : Enable
    Load                                    : Disable
    Device Aware                            : Disable
  CleanAir Event-driven RRM option          : Disabled
  Channel Assignment Leader                 : ewlc-doc (9.12.32.10)
  Last Run                                  : 550 seconds ago

  DCA Sensitivity Level                     : MEDIUM : 10 dB
  DCA Minimum Energy Limit                  : -95 dBm
  Channel Energy Levels
```

```
    Minimum                                 : unknown
    Average                                 : unknown
    Maximum                                 : -128 dBm
  Channel Dwell Times
    Minimum                                 : unknown
    Average                                 : unknown
    Maximum                                 : unknown
  802.11b 2.4 GHz Auto-RF Channel List
    Allowed Channel List                    : 1,6,11
    Unused Channel List                     : 2,3,4,5,7,8,9,10


------------------ show ap dot11 5ghz channel ------------------


Leader Automatic Channel Assignment
  Channel Assignment Mode                   : AUTO
  Channel Update Interval                   : 600 seconds
  Anchor time (Hour of the day)             : 0
  Channel Update Contribution
    Noise                                   : Enable
    Interference                            : Enable
    Load                                    : Disable
    Device Aware                            : Disable
  CleanAir Event-driven RRM option          : Disabled
  Channel Assignment Leader                 : ewlc-doc (9.12.32.10)
  Last Run                                  : 552 seconds ago

  DCA Sensitivity Level                     : MEDIUM : 15 dB
  DCA 802.11n/ac Channel Width              : 20 MHz
  DCA Minimum Energy Limit                  : -95 dBm
  Channel Energy Levels
    Minimum                                 : unknown
    Average                                 : unknown
    Maximum                                 : -128 dBm
  Channel Dwell Times
    Minimum                                 : unknown
    Average                                 : unknown
    Maximum                                 : unknown
  802.11a 5 GHz Auto-RF Channel List
    Allowed Channel List                    :
36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,144,149,153,157,161
    Unused Channel List                     : 165


------------------ show ap dot11 24ghz coverage ------------------


Coverage Hole Detection
  802.11b Coverage Hole Detection Mode            : Enabled
  802.11b Coverage Voice Packet Count             : 100 packet(s)
  802.11b Coverage Voice Packet Percentage        : 50%
  802.11b Coverage Voice RSSI Threshold           : -80 dBm
  802.11b Coverage Data Packet Count              : 50 packet(s)
  802.11b Coverage Data Packet Percentage         : 50%
  802.11b Coverage Data RSSI Threshold            : -80 dBm
  802.11b Global coverage exception level         : 25 %
  802.11b Global client minimum exception level   : 3 clients


------------------ show ap dot11 5ghz coverage ------------------


Coverage Hole Detection
```

```
  802.11a Coverage Hole Detection Mode          : Enabled
  802.11a Coverage Voice Packet Count           : 100 packet(s)
  802.11a Coverage Voice Packet Percentage      : 50 %
  802.11a Coverage Voice RSSI Threshold         : -80dBm
  802.11a Coverage Data Packet Count            : 50 packet(s)
  802.11a Coverage Data Packet Percentage       : 50 %
  802.11a Coverage Data RSSI Threshold          : -80dBm
  802.11a Global coverage exception level       : 25 %
  802.11a Global client minimum exception level : 3 clients


------------------ show ap dot11 24ghz group ------------------


Radio RF Grouping

  802.11b Group Mode               : AUTO
  802.11b Group Update Interval    : 600 seconds
  802.11b Group Leader             : ewlc-doc (9.12.32.10)
  802.11b Last Run                 : 553 seconds ago


RF Group Members

Controller name                   Controller IP
-------------------------------------------------
ewlc-doc                          9.12.32.10



------------------ show ap dot11 5ghz group ------------------


Radio RF Grouping

  802.11a Group Mode               : AUTO
  802.11a Group Update Interval    : 600 seconds
  802.11a Group Leader             : ewlc-doc (9.12.32.10)
  802.11a Last Run                 : 553 seconds ago


RF Group Members

Controller name                   Controller IP
-------------------------------------------------
ewlc-doc                          9.12.32.10



------------------ show ap dot11 24ghz high-density ------------------


------------------ show ap dot11 5ghz high-density ------------------


------------------ show ap dot11 5ghz load-info ------------------


------------------ show ap dot11 24ghz load-info ------------------
```

```
------------------ show ap dot11 24ghz profile ------------------


Default 802.11b AP performance profiles
  802.11b Global Interference threshold    : 10 %
  802.11b Global noise threshold           : -70 dBm
  802.11b Global RF utilization threshold  : 80 %
  802.11b Global throughput threshold      : 1000000 bps
  802.11b Global clients threshold         : 12 clients


------------------ show ap dot11 5ghz profile ------------------


Default 802.11a AP performance profiles

  802.11a Global Interference threshold         : 10 %
  802.11a Global noise threshold                : -70 dBm
  802.11a Global RF utilization threshold       : 80 %
  802.11a Global throughput threshold           : 1000000 bps
  802.11a Global clients threshold              : 12 clients


------------------ show ap dot11 24ghz monitor ------------------


Default 802.11b AP monitoring
  802.11b Monitor Mode                 : Enabled
  802.11b Monitor Channels             : Country channels
  802.11b RRM Neighbor Discover Type   : Transparent
  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
  802.11b NDP RSSI Normalization       : Enabled


------------------ show ap dot11 5ghz monitor ------------------


Default 802.11a AP monitoring
  802.11a Monitor Mode                 : Enabled
  802.11a Monitor Channels             : Country channels
  802.11a RRM Neighbor Discover Type   : Transparent
  802.11a AP Coverage Interval         : 180 seconds
  802.11a AP Load Interval             : 60 seconds
  802.11a AP Noise Interval            : 180 seconds
  802.11a AP Signal Strength Interval  : 60 seconds
  802.11a NDP RSSI Normalization       : Enabled


------------------ 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
    802.11b 11M                               : Mandatory
    802.11g 6M                                : Supported
    802.11g 9M                                : Supported
    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
    MCS 24 : Supported
    MCS 25 : Supported
    MCS 26 : Supported
    MCS 27 : Supported
    MCS 28 : Supported
    MCS 29 : Supported
    MCS 30 : Supported
    MCS 31 : 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
      Aggregation scheduler                   : Enabled
      Realtime timeout                        : 10
    A-MSDU Tx:
      Priority 0                              : Enable
      Priority 1                              : Enable
      Priority 2                              : Enable
      Priority 3                              : Enable
      Priority 4                              : Enable
      Priority 5                              : Enable
      Priority 6                              : Disable
```

```
    Priority 7                              : Disable
  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                             : 1
Default Tx Power Level                      : 1
DTPC Status                                 : Enabled
Call Admission Limit                        :
G711 CU Quantum                             :
ED Threshold                                : -50
Fragmentation Threshold                     : 2346
RSSI Low Check                             : Disabled
RSSI Threshold                              : -127 dbm
PBCC Mandatory                              : unknown
Pico-Cell-V2 Status                         : unknown
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 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 call bandwidth                        : 64
  SIP call bandwith sample-size             : 20
Maximum Number of Clients per AP Radio      : 200


------------------ 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
  MCS 24 : Supported
  MCS 25 : Supported
  MCS 26 : Supported
  MCS 27 : Supported
  MCS 28 : Supported
  MCS 29 : Supported
  MCS 30 : Supported
  MCS 31 : 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
    Aggregation scheduler               : Enabled
    Realtime timeout                    : 10
  A-MSDU Tx:
    Priority 0                          : Enable
    Priority 1                          : Enable
    Priority 2                          : Enable
    Priority 3                          : Enable
    Priority 4                          : Enable
    Priority 5                          : Enable
    Priority 6                          : Disable
    Priority 7                          : Disable
  Guard Interval                        : Any
  Rifs Rx                               : Enabled
802.11ac                                : Enabled
  Frame burst                           : Automatic
802.11ac MCS Settings:
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
```

```
RSSI Low Check                           : Disabled
RSSI Threshold                           : -127 dbm
Pico-Cell-V2 Status                      : unknown
TI Threshold                             :
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 call bandwidth                     : 64
  SIP call bandwith sample-size          : 20
Maximum Number of Clients per AP Radio   : 200


------------------ show ap dot11 24ghz txpower ------------------


Automatic Transmit Power Assignment

Transmit Power Assignment Mode          : AUTO
Transmit Power Update Interval          : 600 seconds
Transmit Power Threshold                : -70 dBm
Transmit Power Neighbor Count           : 3 APs
Min Transmit Power                      : -10 dBm
Max Transmit Power                      : 30 dBm
Update Contribution
    Noise                               : Enable
    Interference                        : Enable
    Load                                : Disable
    Device Aware                        : Disable
Transmit Power Assignment Leader        : ewlc-doc (9.12.32.10)
Last Run                                : 558 seconds ago


------------------ show ap dot11 5ghz txpower ------------------


Automatic Transmit Power Assignment

Transmit Power Assignment Mode          : AUTO
Transmit Power Update Interval          : 600 seconds
Transmit Power Threshold                : -70 dBm
Transmit Power Neighbor Count           : 3 APs
Min Transmit Power                      : -10 dBm
Max Transmit Power                      : 30 dBm
Update Contribution
    Noise                               : Enable
    Interference                        : Enable
    Load                                : Disable
    Device Aware                        : Disable
Transmit Power Assignment Leader        : ewlc-doc (9.12.32.10)
Last Run                                : 558 seconds ago
```

```
------------------ show ap auto-rf dot11 5ghz ------------------


------------------ show ap auto-rf dot11 24ghz ------------------


------------------ show ap config general ------------------



------------------ show ap dot11 5ghz optimized-roaming ------------------

802.11a OptimizedRoaming

  Mode                                  : Disabled
  Reporting Interval                    : 90 seconds
  Rate Threshold                        : Disabled
  Hysteresis                            : 6 db


------------------ show ap rf-profile summary ------------------


Number of RF-profiles: 6

RF Profile Name                  Band     Description                              State
------------------------------------------------------------------------------------------
Low_Client_Density_rf_5gh        5 GHz    pre configured Low Client Density rf Up
High_Client_Density_rf_5gh       5 GHz    pre configured High Client Density r Up
Low_Client_Density_rf_24gh       2.4 GHz  pre configured Low Client Density rf Up
High_Client_Density_rf_24gh      2.4 GHz  pre configured High Client Density r Up
Typical_Client_Density_rf_5gh    5 GHz    pre configured Typical Density rfpro Up
Typical_Client_Density_rf_24gh   2.4 GHz  pre configured Typical Client Densit Up


------------------ show ap fra ------------------

FRA State                                          : Disabled
FRA Sensitivity                                    : medium (95%)
FRA Interval                                       : 1 Hour(s)
  Last Run                                         : 2299 seconds ago
  Last Run time                                    : 0 seconds

AP Name              MAC Address       Slot ID  Current-Band      COF %      Suggested Mode
-----------------------------------------------------------------------------------------------

COF : Coverage Overlap Factor


------------------ 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
```

```
------------------ show wireless  country  configure ------------------


Configured Country.........................   US - United States
Configured Country Codes
        US  - United States                 802.11a Indoor/ 802.11b Indoor/ 802.11g Indoor


------------------ show wireless tag rf summary ------------------


Number of RF Tags: 1

RF tag name                     Description
------------------------------------------------------------------------
default-rf-tag                  default RF tag


------------------ show ap tag summary ------------------

Number of APs: 0


------------------ show ap status ------------------


------------------ show ap uptime ------------------

Number of APs: 0
```

show tunnel eogre global-configuration

To display the Ethernet over GRE (EoGRE) global configuration, use the **show tunnel eogre global-configuration** command.

show tunnel eogre global-configuration

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Example

This example shows how to display the EoGRE global configuration:

```
Device# show tunnel eogre global-configuration

Heartbeat interval       : 60
Max Heartbeat skip count : 3
Source Interface         : (none)
```

show tunnel eogre domain detailed

To display the detailed information of the Ethernet over GRE (EoGRE) tunnel domain, use the **show tunnel eogre domain detailed** command.

show tunnel eogre domain detailed *domain-name*

Syntax Description

domain-name	EoGRE domain name.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Example

This example shows how to display the detailed information of the EoGRE tunnel domain:

```
Device# show tunnel eogre domain detailed eogre_domain

Domain Name    : eogre_domain
 Primary GW    : Tunnel1
 Secondary GW  : Tunnel2
 Active GW     : Tunnel1
 Redundancy    : Non-Revertive
```

show tunnel eogre domain summary

To display the summary information of the Ethernet over GRE (EoGRE) tunnel domain, use the **show tunnel eogre domain summary** command.

show tunnel eogre domain summary

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Example

This example shows how to display the summary information of the EoGRE tunnel domain:

```
Device# show tunnel eogre domain summary

Domain Name          Primary GW   Secondary GW      Active GW      Redundancy
-------------------------------------------------------------------------------
domain1              Tunnel1      Tunnel2           Tunnel1        Non-Revertive
eogre_domain         Tunnel1      Tunnel2           Tunnel1        Non-Revertive
```

show tunnel eogre gateway summary

To display the summary information of the Ethernet over GRE (EoGRE) tunnel gateway, use the **show tunnel eogre gateway summary** command.

show tunnel eogre gateway summary

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Example

This example shows how to display the summary information of the EoGRE tunnel gateway:

```
Device# show tunnel eogre gateway summary

Name               Type  Address                                  AdminState  State  Clients
-------------------------------------------------------------------------------------------
Tunnel1             IPv4  9.51.1.11                                 Up          Up     0

Tunnel2             IPv4  9.51.1.12                                 Up          Down   0

Tunnel10            IPv6  fd09:9:8:21::90                           Down        Down   0

Tunnel11            IPv4  9.51.1.11                                 Up          Up     0

Tunnel12            IPv6  fd09:9:8:21::90                           Up          Down   0

Tunnel100           IPv4  9.51.1.100                                Up          Down   0
```

show tunnel eogre gateway detailed

To display the detailed information of the Ethernet over GRE (EoGRE) tunnel domain, use the **show tunnel eogre gateway detailed** command.

show tunnel eogre gateway detailed *gateway-name*

Syntax Description

gateway-name	EoGRE gateway name.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Example

This example shows how to display the detailed information of the EoGRE tunnel gateway:

```
Device# show tunnel eogre domain detailed Tunnel1

Gateway : Tunnel1
 Mode   : IPv4
 IP     : 9.51.1.11
 Source : Vlan51 / 9.51.1.1
 State  : Up
 SLA ID : 56
 MTU    : 1480
 Up Time: 4 minutes 45 seconds

 Clients
  Total Number of Wireless Clients      : 0
 Traffic
  Total Number of Received Packets      : 0
  Total Number of Received Bytes        : 0
  Total Number of Transmitted Packets   : 0
  Total Number of Transmitted Bytes     : 0
 Keepalives
  Total Number of Lost Keepalives       : 0
  Total Number of Received Keepalives   : 5
  Total Number of Transmitted Keepalives: 5
  Windows                               : 1
  Transmitted Keepalives in last window : 2
  Received Keepalives in last window    : 2
```

show tunnel eogre manager stats global

To display the global tunnel manager statistics, use the **show tunnel eogre manager stats global** command.

show tunnel eogre manager stats global

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Example

This example shows how to display the global tunnel manager statistics:

```
Device# show tunnel eogre manager stats global

Tunnel Global Statistics
Last Updated                    : 02/18/2019 23:50:35
EoGRE Objects
  Gateways                      : 6
  Domains                       : 2

EoGRE Flex Objects
  AP Gateways                   : 2
  AP Domains                    : 1
  AP Gateways HA inconsistencies : 0
  AP Domains HA inconsistencies  : 0

Config events
  IOS Tunnel updates            : 806
  IOS Domain updates            : 88
  Global updates                : 48
  Tunnel Profile updates        : 120
  Tunnel Rule updates           : 16
  AAA proxy key updates         : 0

AP events
  Flex AP Join                  : 1
  Flex AP Leave                 : 0
  Local AP Join                 : 0
  Local AP leave                : 0
  Tunnel status (rx)            : 4
  Domain status (rx)            : 1
  IAPP stats msg (rx)           : 3
  Client count (rx)             : 6
  VAP Payload msg (tx)          : 4
  Domain config (tx)            : 1
  Global config (tx)            : 1
  Client delete (tx)            : 1
```

```
  Client delete per domain (tx)  : 3
  DHCP option 82 (tx)            : 4

Client events
  Add-mobile                     : 2
  Run-State                      : 3
  Delete                         : 1
  Cleanup                        : 0
  Join                           : 2
  Plumb                          : 0
  Join Errors                    : 0
  HandOff                        : 0
  MsPayload                      : 2
  FT Recover                     : 0
  Zombie GW counter increase     : 0
  Zombie GW counter decrease     : 0
  Tunnel Profile reset           : 88
  Client deauth                  : 0
  HA reconciliation              : 0

Client Join Events
  Generic Error                  : 0
  MSPayload Fail                 : 0
  Invalid VLAN                   : 0
  Invalid Domain                 : 0
  No GWs in Domain               : 0
  Domain Shut                    : 0
  Invalid GWs                    : 0
  GWs Down                       : 0
  Rule Match Error               : 0
  AAA-override                   : 0
  Flex No Active GW              : 0
  Open Auth join attempt         : 2
  Dot1x join attempt             : 2
  Mobility join attempt          : 0
  Tunnel Profile not valid       : 2
  Tunnel Profile valid           : 2
  No rule match                  : 0
  Rule match                     : 2
  AAA proxy                      : 0
  AAA proxy accounting           : 0
  AAA eogre attributes           : 0
  Has aaa override               : 0
  Error in handoff payload       : 0
  Handoff AAA override           : 0
  Handoff no AAA override        : 0
  Handoff payload received       : 0
  Handoff payload sent           : 0

SNMP Traps
  Client                         : 0
  Tunnel                         : 2
  Domain                         : 0

IPC
  IOSd TX messages               : 0

Zombie Client
  Entries                        : 0
```

show tunnel eogre manager stats instance

To display the tunnel manager statistics for a specific WNCd instance, use the **show tunnel eogre manager stats instance** command.

show tunnel eogre manager stats instance *instance-number*

Syntax Description

instance-number	WNCd instance number.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Example

This example shows how to display the tunnel manager statistics for a specific WNCd instance:

```
Device# show tunnel eogre manager stats instance 0

Tunnel Manager statistics for process instance : 0
Last Updated                      : 02/18/2019 23:50:35
EoGRE Objects
  Gateways                        : 6
  Domains                         : 2

EoGRE Flex Objects
  AP Gateways                     : 2
  AP Domains                      : 1
  AP Gateways HA inconsistencies  : 0
  AP Domains HA inconsistencies   : 0

Config events
  IOS Tunnel updates              : 102
  IOS Domain updates              : 11
  Global updates                  : 6
  Tunnel Profile updates          : 15
  Tunnel Rule updates             : 2
  AAA proxy key updates           : 0

AP events
  Flex AP Join                    : 1
  Flex AP Leave                   : 0
  Local AP Join                   : 0
  Local AP leave                  : 0
  Tunnel status (rx)              : 4
  Domain status (rx)              : 1
  IAPP stats msg (rx)             : 3
  Client count (rx)               : 6
  VAP Payload msg (tx)            : 4
```

```
  Domain config (tx)             : 1
  Global config (tx)             : 1
  Client delete (tx)             : 1
  Client delete per domain (tx)  : 3
  DHCP option 82 (tx)            : 4

Client events
  Add-mobile                     : 2
  Run-State                      : 3
  Delete                         : 1
  Cleanup                        : 0
  Join                           : 2
  Plumb                          : 0
  Join Errors                    : 0
  HandOff                        : 0
  MsPayload                      : 2
  FT Recover                     : 0
  Zombie GW counter increase     : 0
  Zombie GW counter decrease     : 0
  Tunnel Profile reset           : 11
  Client deauth                  : 0
  HA reconciliation              : 0

Client Join Events
  Generic Error                  : 0
  MSPayload Fail                 : 0
  Invalid VLAN                   : 0
  Invalid Domain                 : 0
  No GWs in Domain               : 0
  Domain Shut                    : 0
  Invalid GWs                    : 0
  GWs Down                       : 0
  Rule Match Error               : 0
  AAA-override                   : 0
  Flex No Active GW              : 0
  Open Auth join attempt         : 2
  Dot1x join attempt             : 2
  Mobility join attempt          : 0
  Tunnel Profile not valid       : 2
  Tunnel Profile valid           : 2
  No rule match                  : 0
  Rule match                     : 2
  AAA proxy                      : 0
  AAA proxy accounting           : 0
  AAA eogre attributes           : 0
  Has aaa override               : 0
  Error in handoff payload       : 0
  Handoff AAA override           : 0
  Handoff no AAA override        : 0
  Handoff payload received       : 0
  Handoff payload sent           : 0

SNMP Traps
  Client                         : 0
  Tunnel                         : 2
  Domain                         : 0

IPC
  IOSd TX messages               : 0

Zombie Client
  Entries                        : 0
```

show wireless band-select

To display the status of the band-select configuration, use the **show wireless band-select** command in privileged EXEC mode.

show wireless band-select

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following is sample output from the **show wireless band-select** command:

```
Device# 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
```

show wireless client

To see the summary of the classified devices, use the **show wireless client** command.

show wireless client device {**cache** | **count** | **summary** } | **{steering**}[{**chassis**{*chassis-number* | **active** | **standby** }}]**R0**

Syntax Description

device	Shows classified devices.
steering	Wireless client steering information
cache	Shows the cached classified device summary.
count	Shows the wireless device count.
summary	Shows the active classified device summary.
chassis-number	Chassis number. Valid range is 1–2.
active	Active instance.
standby	Standby instance.
R0	Route-Processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the summary of the classified devices:

```
Device# show wireless client device summary
```

show wireless client mac-address

To view detailed information of a client using its mac-address, use the **show wireless client mac-addressdetail** command.

show wireless client mac-address *mac-address* **detail** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

mac-address	Client MAC address.
chassis-number	Chassis number. Valid range is 1–2.
active	Active instance.
standby	Standby instance.
R0	Route-Processor slot 0.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

The Client Scan Reports section in the output of the **show wireless client mac-address detail** is populated only for the following Apple devices:

- Any iPhone 7 and running iOS 11.0 or higher
- Any iPad after iPad Pro (1st gen, 12.9-inch, 2015) and running iOS 11.0 or higher

Other client devices, even if it supports 802.11k or is Wi-Fi Agile Multiband (MBO) certified, are not currently supported to populate the Client Scan Reports section.

Client ACLs shown under **show wireless client mac-address** <*mac address*> **detail** are ACLs applied on the client in Flexconnect local authentication case with MAB+Web authentication WLAN with AAA override enabled. This is applicable only for Express Wi-Fi by Facebook Policy on Controller. For more information about Facebook policy, see Express Wi-Fi by Facebook.

From Cisco IOS XE Amsterdam 17.3.1 onwards, the controller retains client session for 10 seconds. This feature is applicable for clients in the RUN state and is supported on central authentication with local and flex mode.

In idle state, 10 sec represents idle state timeout and 09 sec represent remaining time out of 10 sec. An example is given below:

```
Idle state timeout : 10 sec (Remaining time: 09 sec)
```

Examples

The following example shows how to see detailed client information using its MAC address:

```
Device# show wireless client mac-address 98-XX-7B-XX-EF-XX detail
```

show wireless client mac-address (Call Control)

To view call control information related to clients, use the **show wireless client mac-address** command in privileged EXEC mode.

show wireless client mac-address *mac-address* **call-control call-info**

Syntax Description

mac-address	The client MAC address.
call-control call-info	Displays the call control and IP-related information about a client.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
	This command was introduced.

This example shows how to display call control and IP-related information about a client:

```
Device# show wireless client mac-address  30e4.db41.6157 call-control call-info
Client MAC Address        : 30E4DB416157

Call 1 Statistics

Uplink IP Address         : 209.165.200.225
Downlink IP Address       : 209.165.200.226
Uplink Port               : 29052
Downlink Port             : 27538
Call ID                   : c40acb4d-3b3b0.3d27da1e-356bed03
Called Party              : sip:1011
Calling Party             : sip:1012
Priority                  : 6
Call On Hold              : false
Call Duration             : 30

Call 2 Statistics

No Active Call
```

show wireless client mac-address (TCLAS)

To view information about TCLAS and user priority, use the **show wireless client mac-address** command in privileged EXEC mode.

show wireless client mac-address *mac-address* **tclas**

Syntax Description

mac-address	The client MAC address.
tclas	Displays TCLAS and user priority-related information about a client.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to display the TCLAS and user priority-related information about a client:

```
Device# show wireless client mac-address 30e4.db41.6157 tclas
MAC Address      UP TID Mask Source IP Addr  Dest IP Addr    SrcPort DstPort Proto
-------------------------------------------------------------------------------
30e4.db41.6157    4   4   95 167838052       2164326668      5060     5060      6
30e4.db41.6157    6   1   31 0               2164326668      0        27538    17
```

show wireless client summary

To display a summary of active clients associated with the controller, use the **show wireless client summary** command in privileged EXEC mode.

show wireless client summary

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The following is sample output from the **show wireless client summary** command:

Use the **show wireless exclusionlist** command to display clients on the exclusion list.

```
Device# show wireless client summary
Number of Local Clients : 1

MAC Address    AP Name                          WLAN State              Protocol
-------------------------------------------------------------------------------
0000.1515.000f  AP-2                        1    UP                 11a
```

show wireless client timers

To display 802.11 system timers, use the **show wireless client timers** command in privileged EXEC mode.

show wireless client timers

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following is sample output from the **show wireless client timers** command:

```
Device# show wireless client timers
 Authentication Response Timeout (seconds)      : 10
```

show wireless country

To display the configured country and the radio types supported, use the **show wireless country** command in privileged EXEC mode.

show wireless country {**channels** | **configured** | **supported** [**tx-power**]}

Syntax Description

channels	Displays the list of possible channels for each band, and the list of channels allowed in the configured countries.
configured	Display configured countries.
supported tx-power	Displays the list of allowed Tx powers in each supported country.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following is sample output from the **show wireless country channels** command:

```
Device# 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         : . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

The following is sample output from the **show wireless country configured** command:

```
Device# show wireless country configured
 Configured Country.............................: US  - United States
 Configured Country Codes
        US  - United States : 802.11a Indoor,Outdoor/ 802.11b / 802.11g
```

The following is sample output from the **show wireless country supported tx-power** command:

```
Device# show wireless country supported tx-power
      KEY: ##    = Tx Power in dBm.
           ##*   = Channel supports radar detection .
           .     = Channel is not legal in this country.
           (-)   = Regulatory Domains allowed by this country.
           (-,-) = (indoor, outdoor) regulatory Domains 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
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 (-CE  ,-CE  )  AE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  AL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-AR  )  AR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-E   )  AT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-NA  )  AU  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  BA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  BE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  BG  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-    )  BH  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-A   )  BO  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-A   ,-AR  )  BR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  BY  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-ABN )  CA  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-A   ,-ABN )  CA2 :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-E   )  CH  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-AER ,-AR  )  CL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  CM  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-CE  ,-CE  )  CN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-AR  )  CO  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-A   ,-AB  )  CR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-E   )  CY  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  CZ  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  DE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  DK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-ABN )  DO  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  DZ  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-AB  )  EC  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-E   )  EE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  EG  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  ES  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  FI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  FR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  GB  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  GI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  GR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-NA  )  HK  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  HR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  HU  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-ER  )  ID  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  IE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-EI  ,-IE  )  IL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
```

```
(-I   ,-I   )  ILO :   .  .  .  . 20 20 20 20 20 20 20 20 20  .
(-A   ,-AN  )  IN  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  IQ  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  IS  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  IT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-JPU ,-JPU )  J2  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-JPU ,-JPU )  J3  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-JPQU,-PQ  )  J4  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-E   ,-    )  JO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-JPU ,-JPU )  JP  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-ACE ,-ACEK)  KE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  KN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-ACE ,-ACEK)  KR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  KW  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  KZ  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LB  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,     )  LK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LU  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LV  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  MC  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  ME  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  MK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,     )  MO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  MT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-NA  )  MX  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-ACE ,-AEC )  MY  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  NL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  NO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-NA  )  NZ  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  OM  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-AR  )  PA  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AR  )  PE  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-ABN )  PH  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-ABN )  PH2 :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  PK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  PL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-A   )  PR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  PT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-A   )  PY  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  QA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  RO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  RS  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-AER ,-ER  )  RU  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-AE  ,-AE  )  SA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  SE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-SE  )  SG  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E   ,-E   )  SI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  SK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-ER  )  TH  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  TN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-EI  ,-E   )  TR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-ANT )  TW  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  UA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-AB  )  US  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AB  )  US2 :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AB  )  USL :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-    )  USX :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-A   )  UY  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AR  )  VE  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  VN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  ZA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
```

show wireless detail

To display the details of the wireless parameters configured, use the **show wireless detail** command in privileged EXEC mode.

show wireless detail

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

The following parameters are displayed:

- The wireless user idle timeout
- The controller configured RF group name
- Fast SSID change

The following is sample output from the **show wireless detail** command:

```
Device# show wireless detail
User Timeout               : 300
RF network                 : default
Fast SSID                  : Disabled
```

show wireless dot11h

To see 802.11h configuration details, use the **show wireless dot11h** command.

show wireless dot11h [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

chassis-number	Chassis number. Valid range is 1–2.
active	Active instance.
standby	Standby instance.
R0	Route-Processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the 802.11h configuration details:

```
Device# show wireless dot11h
```

show wireless dtls connections

To display the Datagram Transport Layer Security (DTLS) server status, use the **show wireless dtls connections** command in privileged EXEC mode.

show wireless dtls connections

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following is sample output from the **show wireless dtls connections** command:

```
Device# show wireless dtls connections
 AP Name         Local Port   Peer IP    Peer Port  Ciphersuite
------------------------------------------------------------------------
  AP-2       Capwap_Ctrl   10.0.0.16     52346      TLS_RSA_WITH_AES_128_CBC_SHA
  AP-3       Capwap_Ctrl   10.0.0.17     52347      TLS_RSA_WITH_AES_128_CBC_SHA
```

show wireless exclusionlist

To see the wireless exclusion list, use the **show wireless exclusionlist** command.

show wireless exclusionlist [{**client mac-address** *client-mac-addr* **detail** }] [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

client-mac-addr	SI interferers of type microwave oven for the 2.4-GHz band.
chassis-number	Enter the chassis number as either 1 or 2.
active R0	Active instance of the configuration in Route-processor slot 0.
standby R0	Standby instance of the configuration in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the wireless exclusion list:

```
Device# show wireless exclusionlist
```

show wireless load-balancing

To display the status of the load-balancing feature, use the **show wireless load-balancing** command in privileged EXEC mode.

show wireless load-balancing

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following is sample output from the **show wireless load-balancing** command:

```
 > show wireless load-balancing
Aggressive Load Balancing.........................: per WLAN enabling
Aggressive Load Balancing Window (clients)..................:: 5
Aggressive Load Balancing Denial Count.....................:: 3

Statistics
Total Denied Count (clients)................................:: 0
Total Denial Sent (messages)................................:: 0
Exceeded Denial Max Limit Count (times).....................:: 0
None 5G Candidate Count (times).............................:: 0
None 2.4G Candidate Count (times)...........................:: 0
```

show wireless ewc-ap ap summary

To view the embedded wireless controller AP summary , use the **show wireless ewc-ap ap summary** command.

show wireless ewc-ap ap summary [**chassis** {*chassis_number* |**active** | **standby**} {**R0**}]

Syntax Description

ewc-ap	Configures the embedded wireless controller parameters.
ap summary	Displays the embedded wireless controller AP, AP summary.
chassis	Indicates the details of the chassis.
chassis-number	Indicates the chassis number, which is either 1 or 2..
R0	Indicates Route Processor slot 0.
Active	Indicates the active operational mode of the AP chassis.
Standby	Indicates the standby operational mode of the AP chassis.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

The following example shows how to view the embedded wireless controller, AP summary:

```
Device#show wireless ewc-ap ap summary
```

show wireless ewc-ap ap config-sync

To view the embedded wireless controller AP configuration synchronization information or summary, use the **show wireless ewc-ap ap config-sync** command.

show wireless ewc-ap ap config-sync summary [**chassis** {*chassis_number* | **active** | **standby**} {**R0**}]

Syntax Description

config-sync	Configures the embedded wireless controller parameters.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

The following example shows how to view the embedded wireless controller AP configuration synchronization information or summary:

```
Device#show wireless ewc-ap ap config-sync summary
```

show wireless ewc-ap country-code

To view the default country codes and the supported country codes of the embedded wireless controller AP, use the **show wireless ewc-ap country-code** command.

show wireless ewc-ap country-code [**chassis** {*chassis_number* | **active** | **standby**} {**R0**}]

Syntax Description

country-code	Indicates the default country codes and the supported country codes.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

The following example shows how to view the default and supported country codes of embedded wireless controller AP:

```
Device#show wireless ewc-ap country-codes
```

show wireless ewc-ap image-master

To view the image maser information, use the **show wireless ewc-ap image-master** command.

show wireless ewc-ap image-master [**chassis** {*chassis_number* | **active** | **standby**} {**R0**}]

Syntax Description

image-master	Indicates the image master information.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

The following example shows how to view the image master information:

```
Device#show wireless ewc-ap image-master
```

show wireless ewc-ap invalid-image-master

To view the details of the invalid image master, use the **show wireless ewc-ap invalid-image-master** command.

show wireless ewc-ap invalid-image-master [**chassis** {*chassis_number* |**active** | **standby**} {**R0**}]

Syntax Description

invalid-image-master	Indicates the invalid image master information.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

The following example shows how to view the invalid image master information:

```
Device#show wireless ewc-ap invalid-image-master
```

show wireless ewc-ap predownload

To view the image predownload information, use the **show wireless ewc-ap predownload** command.

show wireless ewc-ap predownload {**count** | **status**} [**chassis** {*chassis_number* | **active** | **standby**} {**R0**}]

Syntax Description

predownload	Indicates the image predownload information.
count	Indicates the image predownload count.
status	Indicates the image predownload status.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

The following example shows how to view the image predownload count and status:

```
Device#show wireless ewc-ap predownload
```

show wireless ewc-ap redundancy summary

To view the HA redundancy summary, use the **show wireless ewc-ap redundancy summary** command.

show wireless ewc-ap redundancy summary [**chassis** {*chassis_number* | **active** | **standby**} {**R0**}]

Syntax Description

redundancy	Indicates the HA redundancy information.
summary	Indicates the summary of HA redundancy.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Example

The following example shows how to view the default and supported country codes of embedded wireless controller AP:

```
Device#show wireless ewc-ap redundancy summary
```

show wireless ewc-ap redundancy peers

To view the HA redundancy peers, use the **show wireless ewc-ap redundancy peers** command.

show wireless ewc-ap redundancy peers [**chassis** {*chassis_number* |**active** | **standby**} {**R0**}]

Syntax Description

redundancy	Indicates the HA redundancy information.
peers	Indicates the peers of HA redundancy.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Example

The following example shows how to view the default and supported country codes of embedded wireless controller AP:

```
Device#show wireless ewc-ap redundancy peers
```

show wireless pmk-cache

To display information about the pairwise master key (PMK) cache, use the **show wireless pmk-cache** command in privileged EXEC mode.

show wireless pmk-cache[**mac-address** *mac-addr*]

Syntax Description

mac-address *mac-addr*	(Optional) Information about a single entry in the PMK cache.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following is sample output from the **show wireless pmk-cache mac-address** command:

```
Device# show wireless pmk-cache mac-address H.H.H
Number of PMK caches in total : 0
```

show wireless profile flex

To see the flex parameters of an wireless profile, use the **show wireless profile flex** command.

show wireless profile flex { **detailed** *flex-profile-name* **chassis** {*chassis-number* | **active** | **standby** }**R0** } | **summary chassis** {*chassis-number* | **active** | **standby**}**R0**}

Syntax Description

detailed	Shows the flex-profile detailed parameters
summary	Show the flex-profile summary.
chassis-number	Chassis number. Valid range is 1–2.
active	Active instance.
standby	Standby instance.
R0	Route-Processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the flex parameter's summary of the wireless profile:

```
Device# show wireless profile flex summary
```

show wireless profile policy detailed

To display the wireless policy profile details, use the **show wireless profile policy detailed** command.

show wireless profile policy detailed *policy-profile-name*

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privilege EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

Example

This example displays the wireless policy profile details:

```
Device#show wireless profile policy detailed policy-profile-name
```

show wireless rfid

To display RFID tag information, use the **show wireless rfid** command in privileged EXEC mode.

show wireless rfid {**client** | **detail** *rfid-mac-address* | **stats** | **summary**}

Syntax Description

client	Displays the summary of RFID tags that are clients.
detail	Displays information about a particular RFID tag.
stats	Displays RFID statistics.
summary	Displays summary information for all known RFID tags.
rfid-mac-address	RFID MAC address.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to view RFID information:

```
Device# show wireless rfid summary

Total RFID entries: : 16
Total Unique RFID entries : 16
RFID ID VENDOR Closet AP RSSI Time Since Last Heard
0012.b80a.c791 Cisco 7069.5a63.0520 -31 1 minute 40 seconds ago
0012.b80a.c953 Cisco 7069.5a63.0460 -33 2 minutes 15 seconds ago
0012.b80b.806c Cisco 7069.5a63.0260 -45 22 seconds ago
0012.b80d.e9f9 Cisco 7069.5a63.0460 -38 2 minutes 37 seconds ago
0012.b80d.ea03 Cisco 7069.5a63.0520 -43 2 minutes 38 seconds ago
0012.b80d.ea6b Cisco 7069.5a63.0460 -39 2 minutes 35 seconds ago
0012.b80d.ebe8 Cisco 7069.5a63.0520 -43 1 minute 31 seconds ago
0012.b80d.ebeb Cisco 7069.5a63.0520 -43 2 minutes 37 seconds ago
0012.b80d.ec48 Cisco 7069.5a63.0460 -42 2 minutes 16 seconds ago
0012.b80d.ec55 Cisco 7069.5a63.0520 -41 1 second ago
```

show wireless summary

To display the number of access points, radios and wireless clients known to the controller, use the **show wireless summary** command in privileged EXEC mode.

show wireless summary

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

The following is sample output from the **show wireless summary** command:

```
Device# show wireless summary

Access Point Summary

               Total    Up    Down
---------------------------------
802.11a/n          2     2       0
802.11b/g/n        2     2       0
All APs            2     2       0

Client Summary

Current Clients : 1
Excluded Clients: 0
Disabled Clients: 0
```

show wireless tag rf

To displaye the details of wireless RF tag, use the **show wireless tag rf** command.

show wireless tag rf { **summary** | **detailed***rf-tag-name*

Syntax Description

summary	Disaplys the summary of all RF tags.
detailed	Disaplys details of an RF tag.
rf-tag-name	RF tag name.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows the sample output of **show wireless tag rf summary** command:

```
Device# show  wireless tag rf summary

Number of RF Tags: 1

RF tag name                     Description
------------------------------------------------------------------------
default-rf-tag                  default RF tag
```

show wireless urlfilter details

To view the details of a specified wireless URL filter, use the **show wireless urlfilter details** command.

show wireless urlfilter details *list-name*

Syntax Description

This command has no arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to view the details of a specified wireless URL filter:

```
Device# show wireless urlfilter details urllist_flex_preauth
List Name..................... : urllist_flex_preauth
Filter ID..................... : : 1
Filter Type................... : PRE-AUTH
Action........................ : PERMIT
Redirect server ipv4...... : 8.8.8.8
Redirect server ipv6...... : 2001:0300:0008:0000:0000:0000:0000:0081
Configured List of URLs
   URL........................ : url1.dns.com
```

show wireless urlfilter summary

To view the summary of all wireless URL filters, use the **show wireless urlfilter summary** command.

show wireless urlfilter summary

Syntax Description

This command has no arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to view the summary of all wireless URL filters:

```
Device# show wireless urlfilter summary
Black-list    - DENY
White-list    - PERMIT
Filter-Type   - Specific to Local Mode

URL-List                          ID  Filter-Type  Action   Redirect-ipv4  Redirect-ipv6
-------------------------------------------------------------------------------------------------------
urllist_flex_preauth              1    PRE-AUTH     PERMIT    8.8.8.8
2001:0300:0008:0000:0000:0000:0000:0081
```

show wireless vlan details

To see the VLAN details, use the **show wireless vlan details** command.

show wireless vlan details [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the VLAN details:

```
Device# show wireless vlan details chassis active r0
```

show wireless wgb mac-address

To view all the clients of the wireless workgroup bridge (WGB) using its MAC address, use the **show wireless wgb mac-address** command.

show wireless wgb mac-address *mac-address* **detail**

Syntax Description

mac-address	MAC address of the WGB.
detail	View clients of the wireless WGB.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the clients of the wireless WGB:

```
Device# show wireless wgb mac-address 98-C7-7B-09-EF-ED detail
```

show wireless wgb summary

To see the active workgroup bridges (WGB), use the **show wireless wgb summary** command.

show wireless wgb summary

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to see the active workgroup bridges (WGB):

```
Device# show wireless wgb summary
```

show wireless wps rogue ap summary

To display a list of all rogue access points detected by the switch, use the **show wireless wps rogue ap summary** command.

show wireless wps rogue ap summary

Command Default

None.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None.

This example shows how to display a list of all rogue access points detected by the switch:

```
Device# show wireless wps rogue ap summary
Rogue Location Discovery Protocol            : Disabled
Rogue on wire Auto-Contain                   : Disabled
Rogue using our SSID Auto-Contain            : Disabled
Valid client on rogue AP Auto-Contain        : Disabled
Rogue AP timeout                             : 1200
Rogue Detection Report Interval              : 10
Rogue AP minimum RSSI                        : -128
Rogue AP minimum transient time              : 0

Number of rogue APs detected : 624

MAC Address         Classification     # APs    # Clients   Last Heard
-------------------------------------------------------------------------------------
0018.e78d.250a      Unclassified       1        0           Thu Jul 25 05:04:01 2013
0019.0705.d5bc      Unclassified       1        0           Thu Jul 25 05:16:26 2013
0019.0705.d5bd      Unclassified       1        0           Thu Jul 25 05:10:28 2013
0019.0705.d5bf      Unclassified       1        0           Thu Jul 25 05:16:26 2013
```

show wireless wps rogue client detailed

To view the detailed information of a specific rogue client, use the **show wireless wps rogue client detailed** *client-mac* command.

show wireless wps rogue client detailed *client-mac*

Syntax Description

client-mac	MAC address of the rogue client.

Command Default

None.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None.

This example shows how to display the detailed information for a specific rogue client:

```
Device# show wireless wps rogue client detail  0024.d7f1.2558
Rogue BSSID                       : 64d8.146f.379f
Rogue Radio Type                  : 802.11n - 5GHz
State                             : Alert
First Time Rogue was Reported     : Wed Aug  7 12:51:43 2013
Last Time Rogue was Reported      : Wed Aug  7 12:51:43 2013
Reported by
  AP 2
    MAC Address                   : 3cce.7309.0370
    Name                          : AP3502-talwar-ccie
    Radio Type                    : 802.11a
    RSSI                          : -42 dBm
    SNR                           : 47 dB
    Channel                       : 52
    Last reported by this AP      : Wed Aug  7 12:51:43 2013
```

show wireless wps rogue client summary

To display summary of WPS rogue clients, use the **show wireless wps rogue client summary** command.

show wireless wps rogue client summary

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

Example

The following displays the output of the **show wireless wps rogue client summary** command:

```
Device# show wireless wps rogue client summary
Validate rogue clients against AAA  : Disabled
Validate rogue clients against MSE  : Enabled
Number of rogue clients detected : 0
```

INDEX

C

D

E

F

I

L

M

N

O

P

Q

R

S

T

U

V

W