CHAPTER 50

Configuring SPAN and RSPAN

This chapter describes how to configure the Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) on the Catalyst 4500 series switches. SPAN selects network traffic for analysis by a network analyzer, such as a SwitchProbe device or other Remote Monitoring (RMON) probe.

This chapter consists of the following sections:

Note For complete syntax and usage information for the switch commands used in this chapter, look at the *Cisco Catalyst 4500 Series Switch Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html

If the command is not found in the Catalyst 4500 Command Reference, it is located in the larger Cisco IOS library. Refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products/ps6350/index.html

About SPAN and RSPAN

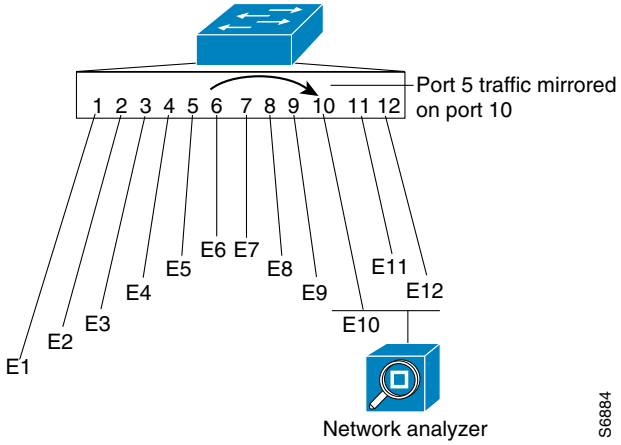
This sections includes the following subsections:

SPAN mirrors traffic from one or more source interfaces on any VLAN or from one or more VLANs to a destination interface for analysis. In Figure 50-1, all traffic on Ethernet interface 5 (the source interface) is mirrored to Ethernet interface 10. A network analyzer on Ethernet interface 10 receives all network traffic from Ethernet interface 5 without being physically attached to it.

For SPAN configuration, the source interfaces and the destination interface must be on the same switch.

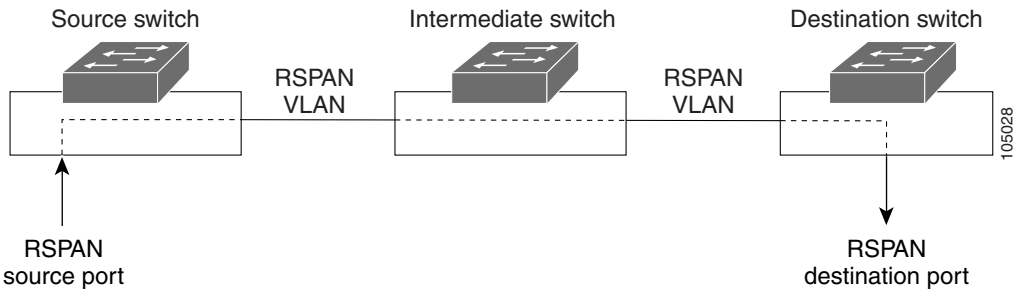
SPAN does not affect the switching of network traffic on source interfaces; copies of the packets received or transmitted by the source interfaces are sent to the destination interface.

Figure 50-1 Example SPAN Configuration



RSPAN extends SPAN by enabling remote monitoring of multiple switches across your network. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The SPAN traffic from the sources is copied onto the RSPAN VLAN and then forwarded over trunk ports that are carrying the RSPAN VLAN to any RSPAN destination sessions monitoring the RSPAN VLAN, as shown in Figure 50-2.

Figure 50-2 Example of RSPAN Configuration



SPAN and RSPAN do not affect the switching of network traffic on source ports or source VLANs; a copy of the packets received or sent by the sources is sent to the destination. Except for traffic that is required for the SPAN or RSPAN session, by default, destination ports do not receive or forward traffic.

Use the SPAN or RSPAN destination port to forward transmitted traffic from a network security device. For example, if you connect a Cisco Intrusion Detection System (IDS) sensor appliance to a destination port, the IDS device can send TCP reset packets to close down the TCP session of a suspected attacker.

SPAN and RSPAN Concepts and Terminology

This section describes concepts and terminology associated with SPAN and RSPAN configuration and includes the following subsections:

SPAN Session

A local SPAN session associates a destination port with source ports. You can monitor incoming or outgoing traffic on a series or range of ports and source VLANs. An RSPAN session associates source ports and source VLANs across your network with an RSPAN VLAN. The destination source is the RSPAN VLAN.

You configure SPAN sessions by using parameters that specify the source of network traffic to monitor.

You can configure multiple SPAN or RSPAN sessions with separate or overlapping sets of SPAN sources. Both switched and routed ports can be configured as SPAN sources or destination ports.

An RSPAN source session associates SPAN source ports or VLANs with a destination RSPAN VLAN. An RSPAN destination session associates an RSPAN VLAN with a destination port.

SPAN sessions do not interfere with the normal operation of the switch; however, an oversubscribed SPAN destination (for example, a 10-Mbps port monitoring a 100-Mbps port) results in dropped or lost packets.

You can configure SPAN sessions on disabled ports; however, a SPAN session does not become active unless you enable the destination port and at least one source port or VLAN for that session.

A SPAN session remains inactive after system startup until the destination port is operational.

Traffic Types

SPAN sessions include these traffic types:

- Receive (Rx) SPAN—The goal of receive (or ingress) SPAN is to monitor as much as possible all packets received by the source interface or VLAN before any modification or processing is performed by the switch. A copy of each packet received by the source is sent to the destination port for that SPAN session. You can monitor a series or range of ingress ports or VLANs in a SPAN session.

On tagged packets (Inter-Switch Link [ISL] or IEEE 802.1Q), the tagging is removed at the ingress port. At the destination port, if tagging is enabled, the packets appear with the ISL or 802.1Q headers. If no tagging is specified, packets appear in the native format.

Packets that are modified because of routing are copied without modification for Rx SPAN; that is, the original packet is copied. Packets that are modified because of quality of service (QoS)—for example, modified Differentiated Services Code Point (DSCP)—are copied without modification for Rx SPAN.

Some features that can cause a packet to be dropped during receive processing have no effect on SPAN; the destination port receives a copy of the packet even if the actual incoming packet is dropped. These features include IP standard and extended input access control lists (ACLs), IP standard and extended output ACLs for unicast and ingress QoS policing, VLAN maps, ingress QoS policing, and policy-based routing. Switch congestion that causes packets to be dropped also has no effect on SPAN.

- Transmit (Tx) SPAN—The goal of transmit (or egress) SPAN is to monitor as much as possible all packets sent by the source interface after the switch performs all modification and processing. After the packet is modified, the source sends a copy of each packet to the destination port for that SPAN session. You can monitor a range of egress ports in a SPAN session.

  Packets that are modified because of routing—for example, with a time-to-live (TTL) or MAC-address modification—are duplicated at the destination port. On packets that are modified because of QoS, the modified packet might not have the same DSCP (IP packet) or CoS (non-IP packet) as the SPAN source.

  Some features that can cause a packet to be dropped during transmit processing might also affect the duplicated copy for SPAN. These features include VLAN maps, IP standard and extended output ACLs on multicast packets, and egress QoS policing. In the case of output ACLs, if the SPAN source drops the packet, the SPAN destination would also drop the packet. In the case of egress QoS policing, if the SPAN source drops the packet, the SPAN destination might not drop it. If the source port is oversubscribed, the destination ports have different dropping behavior.
- Both—In a SPAN session, you can monitor a single port series or a range of ports for both received and sent packets.

Source Port

A source port (also called a *monitored port*) is a switched or routed port that you monitor for network traffic analysis. In a single local SPAN session or RSPAN source session, you can monitor source port traffic, such as received (Rx), transmitted (Tx), or bidirectional (both). The switch supports any number of source ports (up to the maximum number of available ports on the switch) and any number of source VLANs.

A source port has these characteristics:

- It can be any port type (for example, EtherChannel, Fast Ethernet, Gigabit Ethernet, and so forth).
- It can be monitored in multiple SPAN sessions.
- It cannot be a destination port.
- Each source port can be configured with a direction (ingress, egress, or both) to monitor. For EtherChannel sources, the monitored direction would apply to all physical ports in the group.
- Source ports can be in the same or different VLANs.
- For VLAN SPAN sources, all active ports in the source VLAN are included as source ports.

You can configure a trunk port as a source port. By default, all VLANs active on the trunk are monitored. You can limit SPAN traffic monitoring on trunk source ports to specific VLANs by using VLAN filtering. Only switched traffic in the selected VLANs is sent to the destination port. This feature affects only traffic forwarded to the destination SPAN port and does not affect the switching of normal traffic. This feature is not allowed in sessions with VLAN sources.

Destination Port

Each local SPAN session or RSPAN destination session must have a destination port (also called a *monitoring port*) that receives a copy of traffic from the source ports and VLANs.

A destination port has these characteristics:

- A destination port must reside on the same switch as the source port (for a local SPAN session).
- A destination port can be any Ethernet physical port.
- A destination port can participate in only one SPAN session at a time. (A destination port in one SPAN session cannot be a destination port for a second SPAN session.)
- A destination port cannot be a source port.
- A destination port cannot be an EtherChannel group.
- A destination port can be a physical port that is assigned to an EtherChannel group, even if the EtherChannel group has been specified as a SPAN source. The port is removed from the group while it is configured as a SPAN destination port.
- The port does not transmit any traffic except that traffic required for the SPAN session unless learning is enabled. If learning is enabled, the port also transmits traffic directed to hosts that have been learned on the destination port.
- If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.
- A destination port does not participate in spanning tree while the SPAN session is active.
- When it is a destination port, it does not participate in any of the Layer 2 protocols (STP, VTP, CDP, DTP, PagP).
- A destination port that belongs to a source VLAN of any SPAN session is excluded from the source list and is not monitored.
- A destination port receives copies of sent and received traffic for all monitored source ports. If a destination port is oversubscribed, it could become congested and result in packet drops at the destination port. This congestion does not affect traffic forwarding on the source ports.

VLAN-Based SPAN

VLAN-based SPAN (VSPAN) is the monitoring of the network traffic in one or more VLANs.

Use these guidelines for VSPAN sessions:

- Traffic on RSPAN VLANs is not monitored by VLAN-based SPAN sessions.
- Only traffic on the monitored VLAN is sent to the destination port.
- If a destination port belongs to a source VLAN, it is excluded from the source list and is not monitored.
- If ports are added to or removed from the source VLANs, the traffic on the source VLAN received by those ports is added to or removed from the sources being monitored.

- VLAN pruning and the VLAN allowed list have no effect on SPAN monitoring.
- VSPAN monitors only traffic that enters the switch, not traffic that is routed between VLANs. For example, if a VLAN is being Rx-monitored, and the multilayer switch routes traffic from another VLAN to the monitored VLAN, that traffic is not monitored and is not received on the SPAN destination port.
- You cannot use filter VLANs in the same session with VLAN sources.
- You can monitor only Ethernet VLANs.

SPAN Traffic

Use the local SPAN to monitor all network traffic, including multicast and bridge protocol data unit (BPDU) packets, Cisco Discovery Protocol (CDP), VLAN Trunk Protocol (VTP), Dynamic Trunking Protocol (DTP), Spanning Tree Protocol (STP), and Port Aggregation Protocol (PAgP) packets. You cannot use RSPAN to monitor Layer 2 protocols. (See the "RSPAN Configuration Guidelines" section on page 50-16 for more information.)

In some SPAN configurations, multiple copies of the same source packet are sent to the SPAN destination port. For example, a bidirectional (both Rx and Tx) SPAN session is configured for the sources a1 Rx monitor and the a2 Rx and Tx monitor to destination port d1. If a packet enters the switch through a1 and is switched to a2, both incoming and outgoing packets are sent to destination port d1. Both packets are the same (unless a Layer-3 rewrite occurs, in which case the packets are different because of the added Layer 3 information).

SPAN and RSPAN Session Limits

You can configure a maximum of sixteen SPAN/RSPAN sessions (eight concurrent sessions with ingress-only sources and eight concurrent sessions with egress-only sources). Bidirectional sources count as both ingress and egress. RSPAN destination sessions count as a session containing an ingress source.

Default SPAN and RSPAN Configuration

Table 50-1 shows the default SPAN and RSPAN configuration.

Table 50-1 Default SPAN and RSPAN Configuration

Feature	Default Setting
SPAN state	Disabled.
Source port traffic to monitor	Both received and sent traffic (**both**).
Filters	All VLANs, all packet types, all address types.
Encapsulation type (destination port)	Native form (no encapsulation type header).
Ingress forwarding (destination port)	Disabled.
Host learning (destination port)	Disabled.

Configuring SPAN

The following sections describe how to configure SPAN:

Note Entering SPAN configuration commands does not clear previously configured SPAN parameters. You must enter the **no monitor session** command to clear configured SPAN parameters.

SPAN Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when configuring SPAN:

- You must use a network analyzer to monitor interfaces.
- You cannot mix source VLANs and filter VLANs within a SPAN session. You can have source VLANs or filter VLANs, but not both at the same time.
- EtherChannel interfaces can be SPAN source interfaces; they cannot be SPAN destination interfaces.
- When you specify source interfaces and do not specify a traffic type (Tx, Rx, or both), “both” is used by default. To change from both to either “tx” or “rx,” unconfigure the corresponding other type “rx” or “tx” with the **no monitor session** {*session_number*} {**source** {**interface** *interface_list* | {**vlan** *vlan_IDs* | **cpu** [**queue** *queue_ids]* } {**rx** | **tx**} command.
- If you specify multiple SPAN source interfaces, the interfaces can belong to different VLANs.
- You must enter the **no monitor session** *number* command with no other parameters to clear the SPAN session *number*.
- The **no monitor** command clears all SPAN sessions.
- SPAN destinations never participate in any spanning tree instance. SPAN includes BPDUs in the monitored traffic, so any BPDUs seen on the SPAN destination are from the SPAN source.
- SPAN is limited to one destination port per session.
- When you create a SPAN session, the packet filter is set to good by default and you see another configuration line automatically:

  monitor session *number* **filter packet-type good rx**

Configuring SPAN Sources

To configure the source for a SPAN session, perform this task:

Command	Purpose
`Switch(config)# [no] monitor session {session_number} {source {interface <interface_list> | {vlan vlan_IDs | cpu [queue queue_ids] } [rx | tx | both]`	Specifies the SPAN session number (1 through 16), the source interfaces (FastEthernet or GigabitEthernet), VLANs (1 through 4094), whether traffic received or sent from the CPU is copied to the session destination, and the traffic direction to be monitored. For *session_number*, specifies the session number identified with this session (1 through 16). For *interface-list*, specifies the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). For *vlan_IDs*, specifies the source VLAN. For *queue_ids*, specifies the queue(s) involved. (Optional) [**,** | **-**] Specifies a series or range of interfaces. Enter a space after the comma; enter a space before and after the hyphen. (Optional) Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both transmitted (Tx) and received (Rx) traffic. Only received traffic can be monitored on additional source ports. • **Rx**—Monitor received traffic. • **Tx**—Monitor transmitted traffic. • **both**—Monitor both received and transmitted traffic (bidirectional). Queues may be identified either by number or by name. Queue names may subsume multiple numbered queues for convenience. Use the **no** keyword to restore the defaults.

This example shows how to configure SPAN session 1 to monitor bidirectional traffic from source interface Fast Ethernet 5/1:

```
Switch(config)# monitor session 1 source interface fastethernet 5/1
```

This example shows how to configure sources with differing directions within a SPAN session:

```
Switch(config)# monitor session 1 source interface fa2/3 rx
Switch(config)# monitor session 1 source interface fa2/2 tx
Switch(config)#
```

Configuring SPAN Destinations

To configure the destination for a SPAN session, perform this task:

Command	Purpose
`Switch(config)# [no] monitor session <session_number> destination interface <interface> [encapsulation dot1q] [ingress [vlan vlan_IDs] [learning}]`	Specifies the SPAN session number (1 through 16) and the destination interfaces or VLANs. For *session_number*, specifies the session number identified with this session (1 through 16). For *interface*, specifies the destination interface. For *vlan_IDs*, specifies the destination VLAN. Use the **no** keyword to restore the defaults.

Note SPAN is limited to one destination port per session.

This example shows how to configure interface Fast Ethernet 5/48 as the destination for SPAN session 1:

```
Switch(config)# monitor session 1 destination interface fastethernet 5/48
```

Monitoring Source VLANs on a Trunk Interface

To monitor specific VLANs when the SPAN source is a trunk interface, perform this task:

Command	Purpose
`Switch(config)# [no] monitor session {session_number} filter {vlan vlan_IDs [, | - ]} | {packet-type {good | bad}} | {address-type {unicast | multicast | broadcast} [rx | tx | both]}`	Monitors specific VLANs when the SPAN source is a trunk interface. The filter keyword restricts monitoring to traffic that is on the specified VLANs; it is typically used when monitoring a trunk interface. For *session_number*, specifies the session number identified with this session (1 through 16). For *vlan_IDs*, specifies the VLAN. Monitoring is established through all the ports in the specified VLANs Use the **no** keyword to restore the defaults.

This example shows how to monitor VLANs 1 through 5 and VLAN 9 when the SPAN source is a trunk interface:

```
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
```

Configuration Scenario

This example shows how to use the commands described in this chapter to completely configure and unconfigure a span session. Assume that you want to monitor bidirectional traffic from source interfaces Fast Ethernet 4/10, 4/11 and 4/12, Interface 4/10 is configured as a trunk interface carrying VLANs 1 through 4094. Interface Fast Ethernet 4/11 is configured as an access port in VLAN 57 and interface Fast Ethernet 4/12 is configured as an access port in VLAN 58. You want to monitor only traffic in VLAN 57 in that session. Using Fast Ethernet 4/15 as your destination interface, you would enter the following commands:

```
Switch(config)# monitor session 1 source interface fastethernet 4/10 - 12
Switch(config)# monitor session 1 filter vlan 57
Switch(config)# monitor session 1 destination interface fastethernet 4/15
```

You are now monitoring traffic from interface Fast Ethernet 4/10 that is on VLAN 57 out of interface FastEthernet 4/15. To disable the span session enter the following command:

```
Switch(config)# no monitor session 1
```

Verifying a SPAN Configuration

This example shows how to verify the configuration of SPAN session 2:

```
Switch# show monitor session 2
Session 2
---------
Source Ports:
    RX Only:       Fa5/12
    TX Only:       None
    Both:          None
Source VLANs:
    RX Only:       None
    TX Only:       None
    Both:          None
Destination Ports: Fa5/45
Filter VLANs:      1-5,9
Switch#
```

CPU Port Sniffing

When configuring a SPAN session, you can specify the CPU (or a subset of CPU queues) as a SPAN source. Queues may be specified either by number or by name. When such a source is specified, traffic going to the CPU through one of the specified queues is mirrored and sent out of the SPAN destination port in the session. This traffic includes both control packets and regular data packets that are sent to or from the CPU (due to software forwarding).

You can mix the CPU source with either regular port sources or VLAN sources.

To configure CPU source sniffing, perform this task:

Command	Purpose
`Switch(config)# [no] monitor session {session_number} {source {interface interface_list | {vlan vlan_IDs | cpu [queue queue_ids] } [rx | tx | both]`	Specifies that the CPU causes traffic received by or sent from the CPU to be copied to the destination of the session. The **queue** identifier optionally allows sniffing-only traffic (received) on the specified CPU queue(s). For *session_number*, specifies the session number identified with this SPAN session (1 through 16). For *interface-list*, specifies the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). For *vlan_IDs*, specifies the source VLAN. For *queue_ids*, specifies the queue(s) involved. (Optional) [**,** | **-**] Specifies a series or range of interfaces. Enter a space after the comma; enter a space before and after the hyphen. (Optional) Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both transmitted (Tx) and received (Rx) traffic. Only received traffic can be monitored on additional source ports. • **Rx**—Monitor received traffic. • **Tx**—Monitor transmitted traffic. • **both**—Monitor both received and transmitted traffic (bidirectional). Queues may be identified either by number or by name. Queue names may subsume multiple numbered queues for convenience. Use the **no** keyword to restore the defaults.

This example shows how to configure a CPU source to sniff all packets received by the CPU:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# monitor session 1 source cpu rx
```

This example shows how to use queue names and queue number ranges for the CPU as a SPAN source:

```
Switch(config)# monitor session 2 source cpu queue control-packet rx
Switch(config)# monitor session 3 source cpu queue 10 rx
```

Encapsulation Configuration

When configuring a SPAN destination port, you can explicitly enable the encapsulation option. Packets exiting the port are tagged with 802.1q encapsulation. The encapsulation mode also controls how tagged packets are handled when the ingress packet option is enabled.

The replicate encapsulation type (in which packets are transmitted from the destination port using whatever encapsulation applied to the original packet) is not supported. If no encapsulation mode is specified, the port default is untagged. To view the task of configuring encapsulation, see the command table below.

Ingress Packets

When ingress is enabled, the SPAN destination port accepts incoming packets (potentially tagged depending on the encapsulation option) and switches them normally. When configuring a SPAN destination port, you can specify whether the ingress feature is enabled and what VLAN to use to switch untagged ingress packets. Although the port is STP forwarding, it does not participate in the STP, so use caution when configuring this feature lest a spanning-tree loop be introduced in the network. When both ingress and a trunk encapsulation are specified on a SPAN destination port, the port goes forwarding in all active VLANs. Configuring a non-existent VLAN as an ingress VLAN is not allowed.

By default, host learning is disabled on SPAN destination ports with ingress enabled. The port is also removed from VLAN floodsets, so regular traffic is not switched out of the destination port. If learning is enabled, however, then traffic for hosts learned on the destination port is switched out the destination port. A host connected to SPAN destination port will not receive broadcast ARP request and so will not respond. It is also possible to configure static host entries (including a static ARP entry and a static entry in the MAC-address table) on SPAN destination ports.

Note This configuration does not work if the SPAN session does not have a source configured; the session is half configured with only the SPAN destination port.

To configure ingress packets and encapsulation, perform this task:

Command	Purpose
`Switch(config)# [no] monitor session <session_number> destination interface <interface> [encapsulation dot1q] [ingress [vlan vlan_IDs] [learning]]`	Specifies the configuration of the ingress packet and the encapsulation of the destination port. For *session_number*, specifies the session number identified with this SPAN session (1 through 16). For *interface*, specifies the destination interface. For *vlan_IDs*, specifies the destination VLAN. Use the **no** keyword to restore the defaults.

This example shows how to configure a destination port with 802.1q encapsulation and ingress packets using native VLAN 7:

```
Switch(config)# monitor session 1 destination interface fastethernet 5/48
encapsulation dot1q ingress vlan 7
```

With this configuration, traffic from SPAN sources associated with session 1 would be copied out of interface Fast Ethernet 5/48, with 802.1q encapsulation. Incoming traffic would be accepted and switched, with untagged packets being classified into VLAN 7.

Access List Filtering

When configuring a SPAN session, you can apply access list filtering. Access list filtering applies to all packets passing through a SPAN destination port that might be sniffed in the egress or ingress direction. Access list filters are allowed on local SPAN sessions only. If the SPAN destination is an RSPAN VLAN, the access list filter is rejected.

ACL Configuration Guidelines

You can configure ACLs on a SPAN session. Use these guidelines for ACL/SPAN sessions:

- If an ACL is associated with a SPAN session, the rules associated with that ACL are applied against all packets exiting the SPAN destination interface. Rules pertaining to other VACLs or RACLs previously associated with the SPAN destination interface are not applied.
- Only one ACL can be associated with a SPAN session.
- When no ACLs are applied to packets exiting a SPAN destination interface, all traffic is permitted regardless of the PACLs, VACLs, or RACLs that have been previously applied to the destination interface or VLAN to which the SPAN destination interface belongs.
- If an ACL is removed from a SPAN session, all traffic is permitted once again.
- If SPAN configuration is removed from the SPAN session, all rules associated with the SPAN destination interface are applied once again.
- If a SPAN destination port is configured as a trunk port and the VLANs to which it belongs have ACLs associated with them, the traffic is not subjected to the VACLs.
- ACL configuration applies normally to the RSPAN VLAN and to trunk ports carrying the RSPAN VLAN. This configuration enables the user to apply VACLs on RSPAN VLANs. If a user attempts to configure an ACL on a SPAN session with the destination port as an RSPAN VLAN, the configuration is rejected.
- If CAM resources are exhausted and packets are passed to the CPU for lookup, any output port ACLs associated with a SPAN session are not applied.
- If a named IP ACL is configured on a SPAN session before an ACL is created, the configuration is accepted, and the software creates an empty ACL with no ACEs. (An empty ACL permits all packets.) Subsequently, the rules can be added to the ACL.
- The ACLs associated with a SPAN session are applied on the destination interface on output.
- No policing is allowed on traffic exiting SPAN ports.
- Only IP ACLs are supported on SPAN sessions.

Configuring Access List Filtering

To configure access list filtering, perform this task:

Command	Purpose
`Switch(config)# [no] monitor session {session_number} filter {ip access-group [name | id] }{vlan vlan_IDs [, | - ] } | {packet-type {good | bad}} | {address-type {unicast | multicast | broadcast} [rx | tx | both]}`	Specifies filter sniffing based on the access list. For *session_number*, specify the session number identified with this SPAN session (1 through 16). You can specify either a name or a numeric ID for the access list. For *name*, specify the IP access list name. For *id*, specify a standard <1 to 199> or extended <1300-2699> IP access list.

Note IP access lists must be created in configuration mode as described in the chapter "Configuring Network Security with ACLs."

This example shows how to configure IP access group 10 on a SPAN session and verify that an access list has been configured:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# monitor session 1 source interface fa6/1 both
Switch(config)# monitor session 1 destination interface fa6/2
Switch(config)# monitor session 1 filter vlan 1
Switch(config)# monitor session 1 filter ip access-group 10
Switch(config)# exit
Switch# show monitor

Session 1
---------
Type              : Local Session
Source Ports      :
    Both          : Fa6/1
Destination Ports : Fa6/2
    Encapsulation : Native
          Ingress : Disabled
        Learning  : Disabled
Filter VLANs      : 1
IP Access-group   : 10
```

Packet Type Filtering

When configuring a SPAN session, you can specify packet filter parameters similar to VLAN filters. When specified, the packet filters indicate types of packets that may be sniffed. If no packet filters are specified, packets of all types may be sniffed. Different types of packet filters may be specified for ingress and egress traffic.

There are two categories of packet filtering: packet-based (good, error) or address-based (unicast/multicast/broadcast). Packet-based filters can only be applied in the ingress direction. Packets are classified as broadcast, multicast, or unicast by the hardware based on the destination address.

Note When filters of both types are configured, only packets that pass both filters are spanned. For example, if you set both "error" and "multicast," only multicast packets with errors are spanned.

To configure packet type filtering, perform this task:

Command	Purpose
`Switch(config)# [no] monitor session {session_number} filter {vlan vlan_IDs [, | - ] } | {packet-type {good | bad}} | {address-type {unicast | multicast | broadcast} [rx | tx | both]}`	Specifies filter sniffing of the specified packet types in the specified directions. For *session_number*, specifies the session number identified with this SPAN session (1 through 6). For *vlan_IDs*, specifies the VLAN. You can specify both Rx and Tx type filters, as well as specify multiple type filters at the same time (such as **good** and **unicast** to only sniff non-error unicast frames). As with VLAN filters, if no type or filter is specified, then the session sniffs all packet types. Use the **no** keyword to restore the defaults.

This example shows how to configure a session to accept only unicast packets in the ingress direction:

```
Switch(config)# monitor session 1 filter address-type unicast rx
```

Configuration Example

The following is an example of SPAN configuration using some of the SPAN enhancements.

In the example below, you configure a session to sniff unicast traffic arriving on interface Gi1/1. The traffic is mirrored out of interface Gi1/2 with dot1q encapsulation. Ingress traffic is permitted.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# monitor session 1 source interface gi1/1 rx
Switch(config)# monitor session 1 destination interface gi1/2 encapsulation dot1q ingress
Switch(config)# monitor session 1 filter address-type unicast rx
Switch(config)# exit
Switch# show monitor

Session 1
---------
Type              : Local Session
Source Ports      :
    RX Only       : Gi1/1
Destination Ports : Gi1/2
    Encapsulation : DOT1q
          Ingress : Enabled
        Learning  : Disabled
Filter Addr Type  :
    RX Only       : Unicast
```

Configuring RSPAN

This section describes how to configure RSPAN on your switch and it contains this configuration information:

RSPAN Configuration Guidelines

Follow these guidelines when configuring RSPAN:

Note Since RSPAN VLANs have special properties, you should reserve a few VLANs across your network for use as RSPAN VLANs; do not assign access ports to these VLANs.

Note You can apply an output access control list (ACL) to RSPAN traffic to selectively filter or monitor specific packets. Specify these ACLs on the RSPAN VLAN in the RSPAN source switches.

- RSPAN sessions can coexist with SPAN sessions within the limits described in the "SPAN and RSPAN Session Limits" section on page 50-6.
- For RSPAN configuration, you can distribute the source ports and the destination ports across multiple switches in your network.
- RSPAN does not support BPDU packet monitoring or other Layer 2 switch protocols.
- The RSPAN VLAN is configured only on trunk ports and not on access ports. To avoid unwanted traffic in RSPAN VLANs, make sure that all participating switches support the VLAN remote-span feature. Access ports on the RSPAN VLAN are silently disabled.
- You should create an RSPAN VLAN before configuring an RSPAN source or destination session.
- If you enable VTP and VTP pruning, RSPAN traffic is pruned in the trunks to prevent the unwanted flooding of RSPAN traffic across the network for VLAN-IDs that are lower than 1005.
- Because RSPAN traffic is carried across a network on an RSPAN VLAN, the original VLAN association of the mirrored packets is lost. Therefore, RSPAN can only support forwarding of traffic from an IDS device onto a single user-specified VLAN.

Creating an RSPAN Session

First create an RSPAN VLAN that *does not* exist for the RSPAN session in any of the switches that participate in RSPAN. With VTP enabled in the network, you can create the RSPAN VLAN in one switch, and then VTP propagates it to the other switches in the VTP domain for VLAN-IDs that are lower than 1005.

Use VTP pruning to get efficient flow of RSPAN traffic, or manually delete the RSPAN VLAN from all trunks that do not need to carry the RSPAN traffic.

To start an RSPAN source session and to specify the source (monitored) ports and the destination RSPAN VLAN, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# no monitor session {session_number | all | local | remote}`	Clears any existing RSPAN configuration for the session. For *session_number*, specifies the session number identified with this RSPAN session (1 through 16). Specifies **all** to remove all RSPAN sessions, **local** to remove all local sessions, or **remote** to remove all remote SPAN sessions.
Step 3	`Switch(config)# vlan {remote_vlan_ID}`	Specifies a remote VLAN ID. Ensure that the VLAN ID is not being used for any user traffic.
Step 4	`Switch(config-vlan)# remote-span`	Converts the VLAN ID to a remote VLAN ID.
Step 5	`Switch(config-vlan)# exit`	Returns to global configuration mode.
Step 6	`Switch(config)# [no] monitor session {session_number} {source {interface <interface_list> | {vlan vlan_IDs | cpu [queue queue_ids]} [rx | tx | both]`	Specifies the RSPAN session and the source port (monitored port). For *session_number*, specifies the session number identified with this RSPAN session (1 through 16). For *interface-list*, specifies the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). For *vlan-IDs*, specifies the source VLAN or VLANs to monitor. Valid VLANs are in the range from 1 to 4094. For *queue_ids*, specifies either a set of CPU queue numerical identifiers from 1 to 32, or a named queue. (Optional) [**,** | **-**] Specifies a series or range of interfaces. Enter a space after the comma; enter a space before and after the hyphen. (Optional) Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both transmitted (Tx) and received (Rx) traffic. Only received traffic can be monitored on additional source ports. • **Rx**—Monitor received traffic. • **Tx**—Monitor transmitted traffic. • **both**—Monitor both received and transmitted traffic (bidirectional).

	Command	Purpose
Step 7	`Switch(config)# monitor session session_number destination remote vlan vlan-ID`	Specifies the RSPAN session and the destination remote VLAN. For *session_number*, specifies the session number identified with this RSPAN session (1 through 16). For *vlan-ID*, specifies the RSPAN VLAN to carry the monitored traffic to the destination port.
Step 8	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 9	`Switch# show monitor [session session_number]`	Verifies your entries.
Step 10	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

This example shows how to clear any existing RSPAN configuration for session 1, configure RSPAN session 1 to monitor multiple source interfaces, and configure the destination RSPAN VLAN.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface fastEthernet3/10 tx
Switch(config)# monitor session 1 source interface fastEthernet3/2 rx
Switch(config)# monitor session 1 source interface fastEthernet3/3 rx
Switch(config)# monitor session 1 source interface port-channel 102 rx
Switch(config)# monitor session 1 destination remote vlan 901
Switch(config)# end
```

Creating an RSPAN Destination Session

To create an RSPAN destination session and to specify the source RSPAN VLAN and the destination port, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# monitor session session_number source remote vlan vlan-ID`	Specifies the RSPAN session and the source RSPAN VLAN. For *session_number*, specifies the session number identified with this RSPAN session (1 through 16). For *vlan-ID*, specifies the source RSPAN VLAN to monitor.

	Command	Purpose
Step 3	`Switch(config)# [no] monitor session <session_number> destination interface <interface> [encapsulation dot1q] [ingress [vlan vlan_IDs] [learning]]`	Specifies the RSPAN session and the destination interface. For *session_number*, specifies the session number identified with this RSPAN session (1 through 16). For *interface*, specifies the destination interface. For *vlan_IDs*, specifies the ingress VLAN, if necessary. (Optional) [**,** | **-**] Specifies a series or range of interfaces. Enter a space after the comma; enter a space before and after the hyphen. (Optional) Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic. Only received (**rx**) traffic can be monitored on additional source ports.
Step 4	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	`Switch# show monitor [session session_number]`	Verifies your entries.
Step 6	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

This example shows how to configure VLAN 901 as the source remote VLAN and port 5 as the destination interface:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface gigabitEthernet1/2
Switch(config)# end
```

Creating an RSPAN Destination Session and Enabling Ingress Traffic

To create an RSPAN destination session, to specify the source RSPAN VLAN, and to enable ingress traffic on the destination port for a network security device (such as a Cisco IDS [Intrusion Detection System] sensor appliance), perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# monitor session {session_number} source vlan vlan_IDs`	Specifies the RSPAN session and the source RSPAN VLAN. For *session_number*, specifies the session number identified with this RSPAN session (1 through 16). For *vlan_IDs*, specifies the source VLAN or VLANs to monitor. Valid VLANs are in the range from 1 to 4094.

	Command	Purpose
Step 3	`Switch(config)# [monitor session session_number destination interface interface-id [encapsulation dot1q] ingress vlan vlan id] [learning]]`	Specifies the RSPAN session, the destination port, the packet encapsulation, and the ingress VLAN. For *session_number*, specifies the session number identified with this RSPAN session (1 through 16). For *interface-id*, specifies the destination port. Valid interfaces include physical interfaces. (Optional) Specifies the encapsulation of the packets transmitted on the RSPAN destination port. If no encapsulation is specified, all transmitted packets are sent in native format (untagged). • Enter **encapsulation dot1q** to send native VLAN packets untagged, and all other VLAN **tx** packets tagged **dot1q**. (Optional) Specifies whether forwarding is enabled for ingress traffic on the RSPAN destination port. • For native (untagged) and **dot1q** encapsulation, specify **ingress vlan** *vlan id* to enable ingress forwarding with *vlan id* as the native VLAN; *vlan id* is also used as the native VLAN for transmitted packets. • Specify **learning** to enable learning when ingress is enabled.
Step 4	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	`Switch# show monitor [session session_number]`	Verifies your entries.
Step 6	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

This example shows how to configure VLAN 901 as the source remote VLAN and how to configure the destination port for ingress traffic on VLAN 5 by using a security device that supports 802.1Q encapsulation:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface gigabitEthernet1/2 ingress vlan 5
Switch(config)# end
```

Removing Ports from an RSPAN Session

To remove a port as an RSPAN source for a session, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# [no] monitor session {session_number} {source {interface interface_list | {vlan vlan_IDs | cpu [queue queue_ids]} [rx | tx | both]`	Specifies the characteristics of the RSPAN source port (monitored port) to remove. For *session_number*, specifies the session number identified with this RSPAN session (1 through 16). For *interface-list*, specifies the source port to no longer monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). For *vlan_IDs*, specifies the source vlan or vlans to monitor. Valid VLANs are in the range from 1 to 4094. For *queue_ids*, specifies either a set of CPU queue numerical identifiers from 1 to 32, or a named queue. (Optional) [**,** | **-**] Specifies a series or range of interfaces. Enter a space after the comma; enter a space before and after the hyphen. (Optional) Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both transmitted (Tx) and received (Rx) traffic. Only received traffic can be monitored on additional source ports. • **Rx**—Monitor received traffic. • **Tx**—Monitor transmitted traffic. • **both**—Monitor both received and transmitted traffic (bidirectional).
Step 3	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 4	`Switch# show monitor [session session_number]`	Verifies your entries.
Step 5	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

This example shows how to remove port 1 as an RSPAN source for RSPAN session 1:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no monitor session 1 source interface gigabitEthernet1/1
Switch(config)# end
```

This example shows how to disable received traffic monitoring on port 1, which was configured for bidirectional monitoring:

```
Switch(config)# no monitor session 1 source interface gigabitEthernet1/1 rx
```

The monitoring of traffic received on port 1 is disabled, but traffic transmitted from this port continues to be monitored.

Specifying VLANs to Monitor

VLAN monitoring is similar to port monitoring. To specify VLANs to monitor, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# no monitor session {session_number | all | local | remote}`	Clears any existing SPAN configuration for the session. For *session_number*, specifies the session number identified with this RSPAN session (1 through 16). Specify **all** to remove all SPAN sessions, **local** to remove all local sessions, or **remote** to remove all remote SPAN sessions.
Step 3	`Switch(config)# [no] monitor session {session_number} {source {interface interface_list | {vlan vlan_IDs | cpu [queue queue_ids]} [rx | tx | both]`	Specifies the RSPAN session and the source VLANs (monitored VLANs). You can monitor only received (**rx**) traffic on VLANs. For *session_number*, specifies the session number identified with this RSPAN session (1 through 16). For *interface-list*, specifies the source port to no longer monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). For *vlan-IDs*, the range is 1 to 4094; do not enter leading zeros. For *queue_ids*, specifies the source queue. (Optional) **[, | -]** Specifies a series or range of interfaces. Enter a space after the comma; enter a space before and after the hyphen. (Optional) Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both transmitted (Tx) and received (Rx) traffic. Only received traffic can be monitored on additional source ports. • **Rx**—Monitor received traffic. • **Tx**—Monitor transmitted traffic. • **both**—Monitor both received and transmitted traffic (bidirectional).
Step 4	`Switch(config)# monitor session session_number destination remote vlan vlan-id`	Specifies the RSPAN session, the destination remote VLAN. For *session_number*, specifies the session number identified with this RSPAN session (1 through 16). For *vlan-id*, specifies the RSPAN VLAN to carry the monitored traffic to the destination port.
Step 5	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	`Switch# show monitor [session session_number]`	Verifies your entries.
Step 7	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

To remove one or more source VLANs from the RSPAN session, use the **no monitor session** *session_number* **source vlan** *vlan-id* **rx** global configuration command.

This example shows how to clear any existing configuration on RSPAN session 2, configure RSPAN session 2 to monitor received traffic on all ports belonging to VLANs 1 through 3, and send it to destination remote VLAN 902. The configuration is then modified to also monitor received traffic on all ports belonging to VLAN 10.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination remote vlan 902
Switch(config)# monitor session 2 source vlan 10 rx
Switch(config)# end
```

Specifying VLANs to Filter

To limit RSPAN source traffic to specific VLANs, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# no monitor session {session_number | all | local | remote}`	Clears any existing SPAN configuration for the session. For *session_number*, specifies the session number identified with this RSPAN session (1 through 16). Specify **all** to remove all SPAN sessions, **local** to remove all local sessions, or **remote** to remove all remote SPAN sessions.
Step 3	`Switch(config)# [no] monitor session {session_number} {source {interface interface_list | {vlan vlan_IDs | cpu [queue queue_ids]} [rx | tx | both]`	Specifies the characteristics of the source port (monitored port) and RSPAN session. For *session_number*, specifies the session number identified with this RSPAN session (1 through 16). For *interface-list*, specifies the source port to monitor. The interface specified must already be configured as a trunk port. For *vlan-IDs*, the range is 1 to 4094; do not enter leading zeros. For *queue_ids*, specifies the source queue. (Optional) **[, | -]** Specifies a series or range of interfaces. Enter a space after the comma; enter a space before and after the hyphen. (Optional) Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both transmitted (Tx) and received (Rx) traffic. Only received traffic can be monitored on additional source ports. • **Rx**—Monitor received traffic. • **Tx**—Monitor transmitted traffic. • **both**—Monitor both received and transmitted traffic (bidirectional).

	Command	Purpose
Step 4	`Switch(config)# monitor session session_number filter vlan vlan-id [, | -]`	Limits the RSPAN source traffic to specific VLANs. For *session_number*, specifies the session number identified with this RSPAN session (1 through 16). For *vlan-id*, the range is 1 to 4094; do not enter leading zeros. (Optional) Use a comma (**,**) to specify a series of VLANs or use a hyphen (**-**) to specify a range of VLANs. Enter a space after the comma; enter a space before and after the hyphen.
Step 5	`Switch(config)# monitor session session_number destination remote vlan vlan-id`	Specifies the RSPAN session, the destination remote VLAN. For *session_number*, specifies the session number identified with this RSPAN session (1 through 16). For *vlan-id*, specifies the RSPAN VLAN to carry the monitored traffic to the destination port.
Step 6	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	`Switch# show monitor [session session_number]`	Verifies your entries.
Step 8	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

To monitor all VLANs on the trunk port, use the **no monitor session** *session_number* **filter vlan** global configuration command.

This example shows how to clear any existing configuration on RSPAN session 2, configure RSPAN session 2 to monitor traffic received on trunk port 4, and send traffic for only VLANs 1 through 5 and 9 to destination remote VLAN 902.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/1 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination remote vlan 902
Switch(config)# end
```

Displaying SPAN and RSPAN Status

To display the status of the current SPAN or RSPAN configuration, use the **show monitor** privileged EXEC command.

This example displays the output for the **show monitor** command for SPAN source session 1:

```
Switch# show monitor session 1
Session 1
---------
Type: Local Source Session
Source Ports:
    RX Only:  Fa3/13
    TX Only:       None
    Both:          None

Source VLANs:
    RX Only:       None
    TX Only:       None
```

```
    Both:          None
Source RSPAN VLAN: None
Destination Ports: None
    Encapsulation: DOT1Q
    Ingress:Enabled, default VLAN=5
Filter VLANs:      None
Dest RSPAN VLAN: None
Ingress : Enabled, default VLAN=2
Learning : Disabled
```