



Configuring SPAN

This chapter describes how to configure Switched Port Analyzer (SPAN) on your Catalyst 2940 switch.



Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:

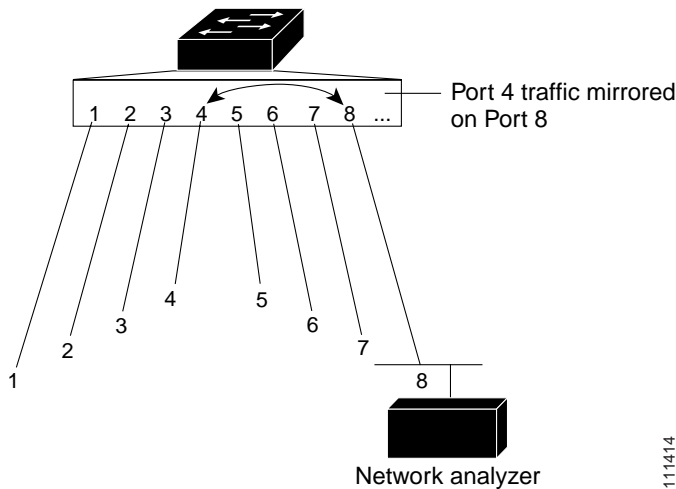
- [Understanding SPAN, page 20-1](#)
- [Configuring SPAN, page 20-5](#)
- [Displaying SPAN Status, page 20-10](#)

Understanding SPAN

You can analyze network traffic passing through ports by using SPAN to send a copy of the traffic to another port on the switch that has been connected to a SwitchProbe device or other Remote Monitoring (RMON) probe or security device. SPAN mirrors received or sent (or both) traffic on one or more source ports to a destination port for analysis.

For example, in [Figure 20-1](#), all traffic on port 4 (the source port) is mirrored to port 8 (the destination port). A network analyzer on port 8 receives all network traffic from port 4 without being physically attached to port 4.

Figure 20-1 Example SPAN Configuration



Only traffic that enters or leaves source ports can be monitored by using SPAN.

You can use the SPAN destination port to inject traffic from a network security device. For example, if you connect a Cisco Intrusion Detection System (IDS) Sensor Appliance to a destination port, the IDS device can send TCP Reset packets to close down the TCP session of a suspected attacker.

SPAN Concepts and Terminology

This section describes concepts and terminology associated with SPAN configuration.

SPAN Session

A local SPAN session is an association of a destination port with source ports. You can monitor incoming or outgoing traffic on a series or range of ports.

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 for that session. The **show monitor session *session_number*** privileged EXEC command displays the operational status of a SPAN session.

A SPAN session remains inactive after system power-on 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 the packets received by the source interface. 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 in a SPAN session.

At the destination port, if tagging is enabled, the packets appear with the 802.1Q header. If no tagging is specified, packets appear in the native format.

Packets that are modified because of —for example, modified Differentiated Services Code Point (DSCP)—are copied with modification for Rx SPAN.

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

For 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. If the source port is oversubscribed, the destination ports will have different dropping behavior.

- **Both**—In a SPAN session, you can monitor a series or range of ports for both received and sent packets.

Source Port

A source port (also called a *monitored port*) is a switched port that you monitor for network traffic analysis. In a single local SPAN 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).

A source port has these characteristics:

- It can be any port type (for example, EtherChannel, Fast Ethernet, Gigabit Ethernet, and so forth).
- 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 the physical ports in the group.
- Source ports can be in the same or different VLANs.

You can configure a trunk port as a source port. All VLANs active on the trunk are monitored.

Destination Port

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

The destination port has these characteristics:

- It must reside on the same switch as the source port.
- It can be any Ethernet physical port.
- It cannot be a source port or a reflector port.
- It cannot be an EtherChannel group or a VLAN.
- It 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 required for the SPAN session.
- If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.

- It 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— Cisco Discovery Protocol (CDP), VLAN Trunk Protocol (VTP), Dynamic Trunking Protocol (DTP), Spanning Tree Protocol (STP), Port Aggregation Protocol (PagP), and Link Aggregation Control Protocol (LACP).
- No address learning occurs on the destination port.
- 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. This could affect traffic forwarding on one or more of the source ports.

SPAN Traffic

You can use SPAN to monitor all network traffic, including multicast and bridge protocol data unit (BPDU) packets, and CDP, VTP, DTP, STP, PagP, and LACP packets.

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.

SPAN Interaction with Other Features

SPAN interacts with these features:

- Spanning Tree Protocol (STP)—A destination port does not participate in STP while its SPAN session is active. The destination port can participate in STP after the SPAN session is disabled. On a source port, SPAN does not affect the STP status.
- Cisco Discovery Protocol (CDP)—A SPAN destination port does not participate in CDP while the SPAN session is active. After the SPAN session is disabled, the port again participates in CDP.
- VLAN and trunking—You can modify VLAN membership or trunk settings for source or destination ports at any time. However, changes in VLAN membership or trunk settings for a destination port do not take effect until you disable the SPAN session. Changes in VLAN membership or trunk settings for a source port immediately take effect, and the SPAN session automatically adjusts accordingly.
- EtherChannel—You can configure an EtherChannel group as a source port but not as a SPAN destination port. When a group is configured as a SPAN source, the entire group is monitored.

If a port is added to a monitored EtherChannel group, the new port is added to the SPAN source port list. If a port is removed from a monitored EtherChannel group, it is automatically removed from the source port list. If the port is the only port in the EtherChannel group, the EtherChannel group is removed from SPAN.

If a physical port that belongs to an EtherChannel group is configured as a SPAN source, or destination port, it is removed from the group. After the port is removed from the SPAN session, it rejoins the EtherChannel group. Ports removed from an EtherChannel group remain members of the group, but they are in the *down* or *standalone* state.

If a physical port that belongs to an EtherChannel group is a destination port and the EtherChannel group is a source, the port is removed from the EtherChannel group and from the list of monitored ports.

- QoS—For ingress monitoring, the packets sent to the SPAN destination port might be different from the packets actually received at the SPAN source port because the packets are forwarded after ingress QoS classification and policing. The packet DSCP might not be the same as the received packet.
- Multicast traffic can be monitored. For egress and ingress port monitoring, only a single unedited packet is sent to the SPAN destination port. It does not reflect the number of times the multicast packet is sent.
- Port security—A secure port cannot be a SPAN destination port.

SPAN Session Limits

You can configure (and store in NVRAM) one local SPAN session on a switch. The SPAN session is restricted to one SPAN source (rx, tx, both) and limited to one active session.

Default SPAN Configuration

Table 20-1 shows the default SPAN configuration.

Table 20-1 Default SPAN Configuration

Feature	Default Setting
SPAN state	Disabled.
Source port traffic to monitor	Both received and sent traffic (both)
Encapsulation type (destination port)	Native form (no encapsulation type header).
Ingress forwarding (destination port)	Disabled.

Configuring SPAN

This section describes how to configure SPAN on your switch. It contains this configuration information:

- [SPAN Configuration Guidelines, page 20-5](#)
- [Creating a SPAN Session and Specifying Ports to Monitor, page 20-6](#)
- [Creating a SPAN Session and Enabling Ingress Traffic, page 20-7](#)
- [Removing Ports from a SPAN Session, page 20-9](#)

SPAN Configuration Guidelines

Follow these guidelines when configuring SPAN:

- The destination port cannot be a source port; a source port cannot be a destination port.
- You can have only one destination port per SPAN session. You cannot have two SPAN sessions using the same destination port.
- An EtherChannel port can be a SPAN source port; it cannot be a SPAN destination port.

- For SPAN source ports, you can monitor sent and received traffic for a single port or for a series or range of ports.
- When you configure a switch port as a SPAN destination port, it is no longer a normal switch port; only monitored traffic passes through the SPAN destination port.
- You can configure a disabled port to be a source or destination port, but the SPAN function does not start until the destination port and at least one source port are enabled.
- A SPAN destination port never participates in any VLAN spanning tree. SPAN does include BPDUs in the monitored traffic, so any spanning-tree BPDUs received on the SPAN destination port for a SPAN session were copied from the SPAN source ports.
- When SPAN is enabled, configuration changes have these results:
 - If you change the VLAN configuration of a destination port, the change is not effective until SPAN is disabled.
 - If you disable all source ports or the destination port, the SPAN function stops until both a source and the destination port are enabled.

Creating a SPAN Session and Specifying Ports to Monitor

Beginning in privileged EXEC mode, follow these steps to create a SPAN session and specify the source (monitored) and destination (monitoring) ports:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	no monitor session { <i>session_number</i> all }	Clear any existing SPAN configuration for the session. For <i>session_number</i> , specify 1. Specify all to remove all SPAN sessions.
Step 3	monitor session <i>session_number</i> source interface <i>interface-id</i> [, -] [both rx tx]	Specify the SPAN session and the source port (monitored port). For <i>session_number</i> , specify 1. For <i>interface-id</i> , specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (port-channel <i>port-channel-number</i>). (Optional) [, -] Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen. (Optional) Specify the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic. <ul style="list-style-type: none"> • both—Monitor both received and sent traffic. • rx—Monitor received traffic. • tx—Monitor sent traffic.

	Command	Purpose
Step 4	monitor session <i>session_number</i> destination interface <i>interface-id</i> [encapsulation { dot1q }]	Specify the SPAN session and the destination port (monitoring port). For <i>session_number</i> , specify 1. For <i>interface-id</i> , specify the destination port. Valid interfaces include physical interfaces. (Optional) Specify the encapsulation header for outgoing packets. If not specified, packets are sent in native form. <ul style="list-style-type: none"> dot1q—Use 802.1Q encapsulation.
Step 5	end	Return to privileged EXEC mode.
Step 6	show monitor [session <i>session_number</i>]	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to set up a SPAN session, session 1, for monitoring source port traffic to a destination port. First, any existing SPAN configuration for session 1 is cleared, and then bidirectional traffic is mirrored from source port 1 to destination port 8.

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface fastethernet0/1
Switch(config)# monitor session 1 destination interface fastethernet0/8
encapsulation dot1q
Switch(config)# end
```

Creating a SPAN Session and Enabling Ingress Traffic

Beginning in privileged EXEC mode, follow these steps to create a SPAN session, to specify the source and destination ports, and to enable ingress traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance):

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	no monitor session { <i>session_number</i> all local }	Clear any existing SPAN configuration for the session. For <i>session_number</i> , specify 1. Specify all or local to remove all SPAN sessions. Though visible in the command-line help, the remote keyword is not supported.

	Command	Purpose
Step 3	monitor session <i>session_number</i> source interface <i>interface-id</i> [, -] [both rx tx]	<p>Specify the SPAN session and the source port (monitored port).</p> <p>For <i>session_number</i>, specify 1.</p> <p>For <i>interface-id</i>, specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (port-channel <i>port-channel-number</i>).</p> <p>(Optional) [, -] Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.</p> <p>(Optional) Specify the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic.</p> <ul style="list-style-type: none"> • both—Monitor both received and sent traffic. • rx—Monitor received traffic. • tx—Monitor sent traffic.
Step 4	monitor session <i>session_number</i> destination interface <i>interface-id</i> [encapsulation { dot1q }] [ingress vlan <i>vlan id</i>]	<p>Specify the SPAN session, the destination port (monitoring port), the packet encapsulation, and the ingress VLAN.</p> <p>For <i>session_number</i>, specify 1.</p> <p>For <i>interface-id</i>, specify the destination port. Valid interfaces include physical interfaces.</p> <p>(Optional) Specify the encapsulation header for outgoing packets. If not specified, packets are sent in native form.</p> <ul style="list-style-type: none"> • dot1q—Use 802.1Q encapsulation. <p>(Optional) Enter ingress vlan <i>vlan id</i> to enable ingress forwarding and specify a default VLAN.</p>
Step 5	end	Return to privileged EXEC mode.
Step 6	show monitor [session <i>session_number</i>]	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that does not support 802.1Q encapsulation.

```
Switch(config)# monitor session 1 destination interface fastethernet0/5 ingress vlan 5
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that supports 802.1Q encapsulation.

```
Switch(config)# monitor session 1 destination interface fastethernet0/5 encapsulation dot1q ingress vlan 5
```

This example shows how to disable ingress traffic forwarding on the destination port.

```
Switch(config)# monitor session 1 destination interface fastethernet0/5 encapsulation dot1q
```

Removing Ports from a SPAN Session

Beginning in privileged EXEC mode, follow these steps to remove a port as a SPAN source for a session:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	no monitor session <i>session_number</i> source interface <i>interface-id</i> [, -] [both rx tx]	Specify the characteristics of the source port (monitored port) and SPAN session to remove. For <i>session</i> , specify 1. For <i>interface-id</i> , specify the source port to no longer monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (port-channel <i>port-channel-number</i>). (Optional) Use [, -] to specify a series or range of interfaces if they were configured. This option is valid when monitoring only received traffic. Enter a space before and after the comma; enter a space before and after the hyphen. (Optional) Specify the direction of traffic (both , rx , or tx) to no longer monitor. If you do not specify a traffic direction, both transmit and receive are disabled.
Step 3	end	Return to privileged EXEC mode.
Step 4	show monitor [session <i>session_number</i>]	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove a source or destination port from the SPAN session, use the **no monitor session** *session_number* **source interface** *interface-id* global configuration command or the **no monitor session** *session_number* **destination interface** *interface-id* global configuration command. To change the encapsulation type back to the default (native), use the **monitor session** *session_number* **destination interface** *interface-id* without the **encapsulation** keyword.

This example shows how to remove a port as a SPAN source for SPAN session 1:

```
Switch(config)# no monitor session 1 source interface fastethernet0/1
Switch(config)# end
```

This example shows how to disable received traffic monitoring on a port that was configured for bidirectional monitoring:

```
Switch(config)# no monitor session 1 source interface fastethernet0/1 rx
```

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

Displaying SPAN Status

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

This is an example of output for the **show monitor** privileged EXEC command for SPAN source session 1:

```
Switch# show monitor session 1
Session 1
-----
Type                : Local Session
Source Ports       :
  RX Only           : None
  TX Only           : None
  Both              : Fa0/4
Source VLANs       :
  RX Only           : None
  TX Only           : None
  Both              : None
Destination Ports  : Fa0/5
Encapsulation: DOT1Q
  Ingress: Enabled, default VLAN = 5
Filter VLANs       : None
```