CHAPTER 20

Configuring SPAN

This chapter describes how to configure Switch Port Analyzer (SPAN) on your switch.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 2950 Desktop Switch Command Reference* for this release.

This chapter consists of these sections:

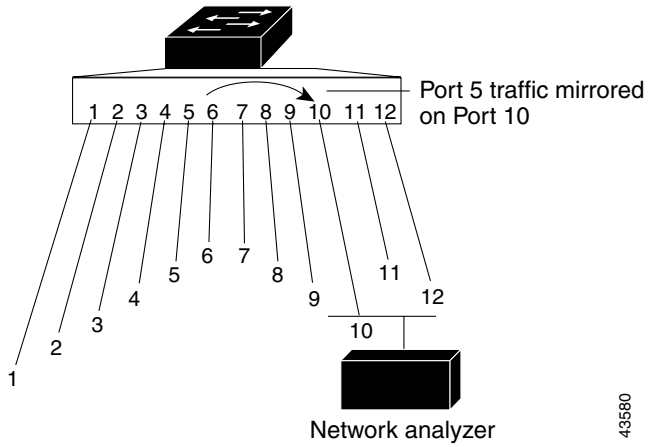
- Understanding SPAN, page 20-1
- Configuring SPAN, page 20-5
- Displaying SPAN Status, page 20-8

Understanding SPAN

You can analyze network traffic passing through ports or VLANs 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. 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 Fast Ethernet port 5 (the source port) is mirrored to Fast Ethernet port 10 (the destination port). A network analyzer on port 10 receives all network traffic from port 5 without being physically attached to port 5.

Figure 20-1 Example SPAN Configuration



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

This release supports only local SPAN, which means the source and destination interfaces must be on the same switch.

SPAN does not affect the switching of network traffic on source ports; a copy of the packets received or sent by the source interfaces are sent to the destination interface. However, an oversubscribed SPAN destination, for example, a 10-Mbps port monitoring a 100-Mbps port, can cause congestion on the switch. Destination ports do not receive or forward traffic, except that required for the SPAN session.

SPAN Concepts and Terminology

This section describes concepts and terminology associated with SPAN configuration.

SPAN Session

A 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.

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. 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, the packets are seen with the 802.1Q tag, but packets from the switch CPU to the destination port are without the 802.1Q tag.

Packets that are modified because of quality of service (QoS)—for example, modified Differentiated Services Code Point (DSCP)—are copied with 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) and IP standard and extended output ACLs for unicast and ingress QoS policing. 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 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.

  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 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. If the source port is oversubscribed, the destination ports will have different dropping behavior.
- Both—In a SPAN session, a series or range of ports can be monitored 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 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 on a trunk source port.

Destination Port

A 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.

- It cannot be an EtherChannel port.
- When it is active, incoming traffic is disabled; it does not forward any traffic except that required for the SPAN session.
- It does not participate in spanning tree while the SPAN session is active.
- When it is an active destination port, it does not participate in any of the Layer 2 protocols (STP, VTP, CDP, DTP, PagP).
- No address learning occurs on the destination port.

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, and PagP 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 sources a1 and a2 to a 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.

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.

Caution Make sure there are no potential loops in the network topology when you enable incoming traffic for a destination port.

- 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 and 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 sessions automatically adjust accordingly.
- EtherChannel—You can configure an EtherChannel group as a source port but not as a SPAN destination port. SPAN configuration fails if the destination port is part of an EtherChannel group. When a channel 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 EtherChannel group. After the port is removed from the SPAN session, it rejoins the EtherChannel group.

- 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.

Configuring SPAN

This section describes how to configure SPAN on your switch and contains this information:

- SPAN Configuration Guidelines, page 20-5
- Creating a SPAN Session and Specifying Ports to Monitor, page 20-6
- Removing Ports from a SPAN Session, page 20-7
- Displaying SPAN Status, page 20-8

SPAN Configuration Guidelines

Follow these guidelines when configuring SPAN:

- SPAN is disabled by default.
- Use a network analyzer to monitor ports.
- Only one SPAN sessions can be active on a switch at the same time.
- The destination port cannot be a source port; a source port cannot be a destination port.
- You can have only one destination port.
- An EtherChannel port can be a SPAN source port; it cannot be a SPAN destination port.
- For a SPAN source port, you can monitor transmitted 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.
- When you specify a single source port and do not specify a traffic type (Tx, Rx, or both), **both** is the default.
- 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 is enabled.
- The **no monitor session** *session_number* global configuration command removes a source or destination port from the SPAN session from the SPAN session. If you do not specify any options following the **no monitor session** *session_number* command, the entire SPAN session is removed.
- 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 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	**monitor session** *session_number* **source interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**]	Specify the SPAN session and the source port (monitored port). For *session_number*, specify 1. For *interface-id*, specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). (Optional) [**,** | **-**] —Specify a series or range of interfaces. This option is valid when monitoring only received traffic. Enter a space 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 transmitted and received traffic. • **both**—Monitor both received and transmitted traffic. • **rx**—Monitor received traffic. • **tx**—Monitor transmitted traffic.
Step 3	**monitor session** *session_number* **destination interface** *interface-id*	Specify the SPAN session and the destination port (monitoring port). For *session_number*, specify 1. For *interface-id*, specify the destination port. Valid interfaces include physical interfaces.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show monitor** [**session** *session_number*]	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove the entire SPAN session, use the **no monitor session** *session_number* global configuration command. 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.

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 2.

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet0/1
Switch(config)# monitor session 1 destination interface gigabitethernet0/2
Switch(config)# end
Switch# show monitor session 1
Session 1
---------
Source Ports:
    RX Only:       None
    TX Only:       None
    Both:          Gi0/1
Destination Ports: Gi0/2
```

Use the **show monitor session** privileged EXEC command to verify the configuration.

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** *session_number* **source interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**]	Specify the characteristics of the source port (monitored port) and SPAN session to remove. For *session*, specify 1. For *interface-id*, specify the source port to no longer monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). (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 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** *session_number*]	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove a destination port from the SPAN session, use the **no monitor session** *session_number* **destination interface** *interface-id* global configuration command.

This example shows how to remove port 1 as a SPAN source for SPAN session 1 and to verify the configuration:

```
Switch(config)# no monitor session 1 source interface gigabitethernet0/1
Switch(config)# end
Switch# show monitor session 1
Session 1
---------
Source Ports:
    RX Only:       None
    TX Only:       None
    Both:          None
Destination Ports:Gi0/2
```

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 gigabitethernet0/1 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 SPAN configuration, use the **show monitor** privileged EXEC command.

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

```
Switch# show monitor session 1
Session 2
---------
Source Ports:
    RX Only:       Gi0/1
    TX Only:       None
    Both:          None
Destination Ports:Gi0/2
```