



Configuring SPAN

This chapter describes how to configure the Switched Port Analyzer (SPAN) feature on the Catalyst 4000 family switch. 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 5 sections:

- [Overview of SPAN, page 24-1](#)
- [SPAN Configuration Guidelines and Restrictions, page 24-4](#)
- [Configuring SPAN, page 24-4](#)



Note

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Cisco IOS Command Reference for the Catalyst 4000 Family Switch* and the publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

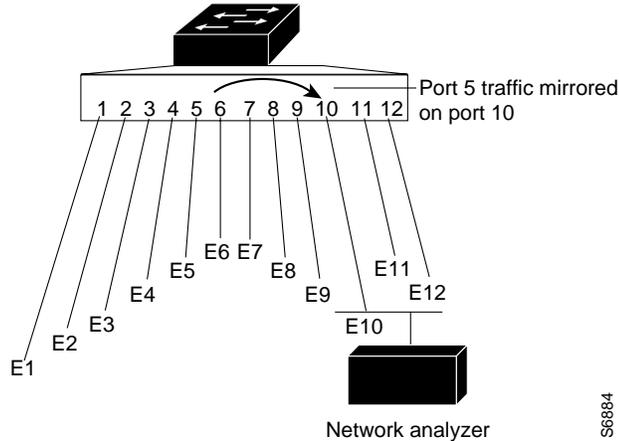
Overview of SPAN

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 24-1](#), 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 24-1 Example SPAN Configuration



S6884

The following sections describe how SPAN works:

- [SPAN Session, page 24-2](#)
- [Destination Interface, page 24-2](#)
- [Source Interface, page 24-3](#)
- [Traffic Types, page 24-3](#)
- [VLAN-Based SPAN, page 24-3](#)
- [SPAN Traffic, page 24-4](#)

SPAN Session

A SPAN session is an association of a destination interface with a set of source interfaces; you configure SPAN sessions using parameters that specify the type of network traffic to monitor. SPAN sessions allow you to monitor traffic on one or more interfaces, or one or more VLANs, and send either ingress traffic, egress traffic, or both to a destination interface.

You can configure up to six separate SPAN sessions (2 ingress, 4 egress) with separate or overlapping sets of SPAN source interfaces or VLANs. A bi-directional SPAN session counts as both 1 ingress and 1 egress session. Both switched and routed interfaces can be configured as SPAN sources.

SPAN sessions do not interfere with the normal operation of the switch. When enabled, a SPAN session might become active or inactive based on various events or actions; a syslog message indicates this. The **show monitor session** command displays the operational status of a SPAN session.

A SPAN session will remain inactive after system boot-up until the destination interface is operational.

Destination Interface

A destination interface (also called a *monitor interface*) is a switched or routed interface where SPAN sends packets for analysis. Once an interface becomes an active destination interface, incoming traffic is disabled. You cannot configure a SPAN destination interface to receive ingress traffic. The interface does not forward any traffic except that required for the SPAN session.

An interface specified as a destination interface in one SPAN session cannot be a destination interface for another SPAN session. An interface configured as a destination interface cannot be configured as a source interface. EtherChannel interfaces cannot be SPAN destination interfaces.

Specifying a trunk interface as a SPAN destination interface stops trunking on the interface.

Source Interface

A source interface is an interface monitored for network traffic analysis. One or more source interfaces can be monitored in a single SPAN session with user-specified traffic types (ingress, egress, or both) applicable for all the source interfaces. All sources for a particular SPAN session are spanned in the same direction.

You can configure source interfaces for any VLAN. You can configure VLANs as source interfaces, which means that all interfaces in the specified VLANs are source interfaces for the SPAN session.

Trunk interfaces can be configured as source interfaces and can be mixed with nontrunk source interfaces; however, the destination interface never encapsulates, so you do not see any encapsulation out of the SPAN destination interface.

Traffic Types

Ingress SPAN (Rx) copies network traffic received by the source interfaces for analysis at the destination interface. Egress SPAN (Tx) copies network traffic transmitted from the source interfaces. Specifying the configuration option “both” copies network traffic received and transmitted by the source interfaces to the destination interface.

VLAN-Based SPAN

VLAN-based SPAN analyzes the network traffic in one or more VLANs. You can configure VLAN based-SPAN as ingress SPAN, egress SPAN, or both. All of the interfaces in the source VLANs become source interfaces for the VLAN-based SPAN session.

Use the following guidelines for VLAN-based SPAN sessions:

- Trunk interfaces are included as source interfaces for VLAN-based SPAN sessions.
- For VLAN-based SPAN sessions with both ingress and egress SPAN configured, two packets are forwarded by the SPAN destination interface if the packets get switched on the same VLAN.
- When a VLAN is cleared, it is removed from the source list for VLAN-based SPAN sessions.
- Inactive VLANs are not allowed for VLAN-based SPAN configuration.
- If a VLAN is being ingress monitored and the switch routes traffic from another VLAN to the monitored VLAN, that traffic is not monitored—it is not seen on the SPAN destination interface. Additionally, traffic that gets routed from an egress-monitored VLAN to some other VLAN does not get monitored. VLAN-based SPAN only monitors traffic that leaves or enters the switch, not traffic that gets routed between VLANs.

SPAN Traffic

All network traffic, including multicast and bridge protocol data unit (BPDU) packets, can be monitored using SPAN.

In some SPAN configurations, multiple copies of the same source packet are sent to the SPAN destination interface. For example, a bidirectional (both ingress and egress) SPAN session is configured for sources a1 and a2 to a destination interface d1. If a packet enters the switch through a1 and gets switched to a2, both incoming and outgoing packets are sent to destination interface d1; both packets would be the same (unless a Layer-3 rewrite had occurred, in which case the packets would be different).

SPAN Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when configuring SPAN:

- 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.
- If you specify multiple SPAN source interfaces, the interfaces can belong to different VLANs.
- 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.
- You cannot configure a SPAN destination interface to receive ingress traffic.
- 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.

Configuring SPAN

The following sections describe how to configure SPAN:

- [Configuring SPAN Sources, page 24-5](#)
- [Configuring SPAN Destinations, page 24-5](#)
- [Monitoring Source VLANs on a Trunk Interface, page 24-6](#)
- [Configuration Scenario, page 24-6](#)
- [Verifying a SPAN Configuration, page 24-6](#)



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.

Configuring SPAN Sources

To configure the source for a SPAN session, enter the following command:

Command	Purpose
Switch(config)# [no] monitor session {session_number} {source {interface type/num} {vlan vlan_ID}} [, - rx tx both]	Specifies the SPAN session number (1 through 6), the source interfaces (FastEthernet or GigabitEthernet), or VLANs (1 through 1005), and the traffic direction to be monitored. 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, enter the following command:

Command	Purpose
Switch(config)# [no] monitor session {session_number} {destination {interface type/num} }	Specifies the SPAN session number (1 through 6) and the destination interfaces or VLANs. Use the no keyword to restore the defaults.

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, enter the following command:

Command	Purpose
Switch(config)# [no] monitor session {session_number} {filter vlan {vlan_ID} [, -]}	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. 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 interface Fast Ethernet 4/10, which is configured as a trunk interface carrying VLANs 1 through 1005. Moreover, you want to monitor only traffic in VLAN 57 on that trunk. 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
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#
```