Configuring Switched Port Analyzer

- Restrictions for Switched Port Analyzer, on page 1
- Information about Switched Port Analyzer, on page 2
- Switched Port Analyzer Configuration Guidelines, on page 3
- How to Configure Switched Port Analyzer, on page 3
- Monitoring Switched Port Analyzer Operations, on page 6
- Configuration Examples for Local Switched Port Analyzer, on page 6
- Feature Information for Switched Port Analyzer, on page 7

Restrictions for Switched Port Analyzer

The restrictions for the Switched Port Analyzer (SPAN) are as follows:

- SPAN filtering is not supported.
- For SPAN sources, you can monitor traffic for a single port or a series or range of ports for each session.
- The destination port cannot be a source port; a source port cannot be a destination port.
- You cannot have two SPAN sessions using the same destination port.
- You cannot have two SPAN sessions using the same source port.
- 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.
- Entering SPAN configuration commands does not remove previously configured SPAN parameters. You must enter the **no monitor session** *session_number* global configuration command to delete configured SPAN parameters.
- 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.

Traffic monitoring in a SPAN session has the following restrictions:

- The device supports up to four local SPAN sessions.
- SPAN sessions do not interfere with the normal operation of the device. However, an oversubscribed SPAN destination, for example, a 10-Mb/s port monitoring a 100-Mb/s port, can result in dropped or lost packets.

- When SPAN is enabled, each packet being monitored is sent twice, once as normal traffic and once as a monitored packet. Monitoring a large number of ports could potentially generate large amounts of network traffic.
- 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.

Information about Switched Port Analyzer

This section provides information about SPAN.

Switched Port Analyzer

You can analyze network traffic passing through ports by using SPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN session, destination ports do not receive or forward traffic.

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.

Note We recommend that you do not use SPAN with multiple source ports. If there are multiple source ports, it is not guaranteed that all mirrored traffic will be captured at the destination port.

Default Switched Port Analyzer Configuration

Table 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 (untagged packets).
Ingress forwarding (destination port)	Disabled.

Switched Port Analyzer Configuration Guidelines

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. For destination interfaces, the **encapsulation** options are ignored with the **no** form of the command.

How to Configure Switched Port Analyzer

This section provides information about how to configure SPAN.

Creating a Local Switched Port Analyzer Session

Follow these steps to create a SPAN session and specify the source (monitored) ports or VLANs and the destination (monitoring) ports.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**no monitor session** *session_number* **Example:** `Device(config)# no monitor session 1`	Removes existing SPAN configuration for the specified session. The range is 1 to 4.
Step 4	**monitor session** *session_number* **source** {**interface** *interface-id*} [**,** | **-**] [**both** | **rx** | **tx**] **Example:** `Device(config)# monitor session 1 source interface gigabitethernet 1/0/1`	Specifies the SPAN session and the source port (monitored port). • For *session_number*, the range is 1 to 4. • For *interface-id*, specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). Valid port-channel numbers are 1 to 6.

	Command or Action	Purpose

		• (Optional) [**,** | **-**]: Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.
		• (Optional) **both** | **rx** | **tx**: Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic.
		  • **both**: Monitors both received and sent traffic.
		  • **rx**: Monitors received traffic.
		  • **tx**: Monitors sent traffic.
		  Note You can use the **monitor session** *session_number* **source** command multiple times to configure multiple source ports.

Step 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] } **Example:** `Device(config)# monitor session 1 destination interface gigabitethernet 1/0/2`	Specifies the SPAN session and the destination port (monitoring port). The port LED changes to amber when the configuration changes take effect. The LED returns to its original state(green) only after removing the SPAN destination configuration. **Note** For local SPAN, you must use the same session number for the source and destination interfaces. • For *session_number*, specify the session number entered in step 4. • For *interface-id*, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN. • (Optional) [**,** | **-**] Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen. **Note** You can use **monitor session** *session_number* **destination** command multiple times to configure multiple destination ports.

	Command or Action	Purpose
Step 6	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Creating a Local Switched Port Analyzer Session and Configuring Incoming Traffic

Follow these steps to create a SPAN session, to specify the source ports or VLANs and the destination ports, and to enable incoming traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**no monitor session** *session_number* **Example:** `Device(config)# no monitor session 1`	Removes existing SPAN configuration for the specified session. The range is 1 to 4.
Step 4	**monitor session** *session_number* **source** {**interface** *interface-id*} [**,** | **-**] [**both** | **rx** | **tx**] **Example:** `Device(config)# monitor session 2 source interface gigabitethernet 1/0/1 rx`	Specifies the SPAN session and the source port (monitored port).
Step 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [**encapsulation replicate ingress** {**vlan** *vlan-id*} | **ingress** {**vlan** *vlan-id*}]} **Example:**	Specifies the SPAN session, the destination port, the packet encapsulation, and the ingress VLAN and encapsulation. • For *session_number*, specify the session number entered in Step 4.

	Command or Action	Purpose
	`Device(config)# monitor session 2 destination interface gigabitethernet 1/0/1 ingress vlan 6`	• For *interface-id*, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN. • (Optional) **encapsulation replicate**: Specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged). • **ingress**: Enables forwarding of incoming traffic on the destination port and to specify the encapsulation type.
Step 6	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Monitoring Switched Port Analyzer Operations

The following table describes the command used to display SPAN operations configuration and results to monitor operations:

Table 2: Monitoring SPAN Operations

Command	Purpose
show monitor session	Displays the current SPAN configuration. Enter the **all** keyword to show configuration for all SPAN sessions, the **local** keyword to show configurations for local sessions only, and the **range** keyword to show configurations for a range of SPAN sessions.

Configuration Examples for Local Switched Port Analyzer

This example shows how to set up SPAN session 1 for monitoring source port traffic to a destination port. First, any existing SPAN configuration for session 1 is deleted, and then bidirectional traffic is mirrored from source Gigabit Ethernet port 1 to destination Gigabit Ethernet port 2, retaining the encapsulation method.

```
Device> enable
Device# configure terminal
```

```
Device(config)# no monitor session 1
Device(config)# monitor session 1 source interface gigabitethernet 1/0/1
Device(config)# monitor session 1 destination interface
Device(config)# end
```

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

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1 source interface gigabitethernet 1/0/1
Device(config)# end
```

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

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1 source interface gigabitethernet 1/0/1 rx
```

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

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor received traffic on all ports belonging to VLANs 1 through 3, and send it to destination Gigabit Ethernet port 2. The configuration is then modified to also monitor all traffic on all ports belonging to VLAN 10.

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 destination interface gigabitethernet 1/0/2
Device(config)# end
```

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor received traffic on Gigabit Ethernet source port 1, and send it to destination Gigabit Ethernet port 2 with the same egress encapsulation type as the source port, and to enable ingress forwarding with VLAN 6 as the default ingress VLAN:

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source gigabitethernet 1/0/1 rx
Device(config)# monitor session 2 destination interface gigabitethernet 1/0/2 encapsulation
 replicate ingress vlan 6
Device(config)# end
```

Feature Information for Switched Port Analyzer

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS Release 15.2(7)E3k	Switch Port Analyzer (SPAN)	SPAN allows to analyze network traffic on ports by sending copies of the traffic to either another port on the switch or onto another switch that has been connected to a network analyzer or other monitoring or security device.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.