Configuring SPAN

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

Restrictions for SPAN

SPAN

The restrictions for SPAN are as follows:

- • 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.

- • When you configure a device port as a SPAN destination port, it is no longer a normal device port; only monitored traffic passes through the SPAN destination port. The switch also supports ingress learning.

- 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 is enabled.

Traffic monitoring in a SPAN session has the following restrictions:

- The device supports only one local SPAN session.

- 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 SPAN

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 device or on another device 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.

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.

Local SPAN

Local SPAN supports a SPAN session entirely within one switch; all source ports and destination ports are in the same switch. Local SPAN copies traffic from one or more source ports to a destination port for analysis.

Figure 1: Example of Local SPAN Configuration on a Single Device

All traffic on port 5 (the source port) is mirrored to 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.
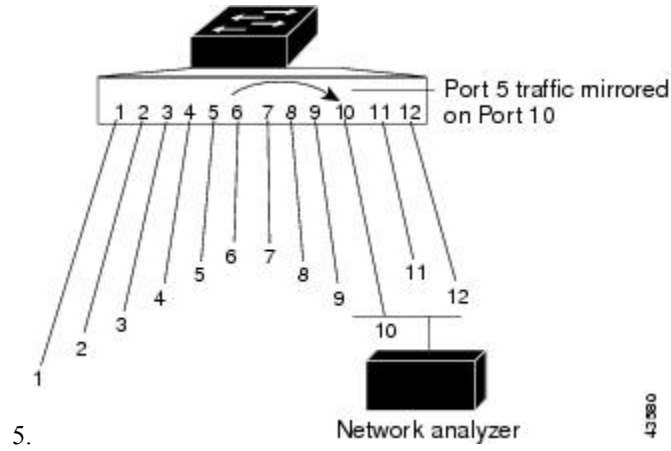
SPAN Concepts and Terminology

•

SPAN Sessions

A local SPAN session is an association of a destination port with source ports, all on a single network device. Local SPAN does not have separate source and destination sessions. Local SPAN sessions gather a set of ingress and egress packets specified by the user and form them into a stream of SPAN data, which is directed to the destination port.

Traffic monitoring in a SPAN session has these restrictions:

- 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. Therefore 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.

Note   The Cisco Digital Building switch supports local SPAN only; remote SPAN (RSPAN) is not supported. Also, the switch supports SPAN for switch ports only; VLAN-based SPAN (VSPAN) is not supported.

Monitored Traffic

SPAN sessions can monitor these traffic types:

- Receive (Rx) SPAN—Receive (or ingress) SPAN monitors as much as possible all of the packets received by the source interface or VLAN before any modification or processing is performed by the device. A copy of each packet received by the source is sent to the destination port for that SPAN session.

  Packets that are modified because of routing or Quality of Service (QoS)—for example, modified Differentiated Services Code Point (DSCP)—are copied before modification.

  Features that can cause a packet to be dropped during receive processing have no effect on ingress 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), ingress QoS policing, VLAN ACLs, and egress QoS policing.

- Transmit (Tx) SPAN—Transmit (or egress) SPAN monitors as much as possible all of the packets sent by the source interface after all modification and processing is performed by the device. 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.

  Packets that are modified because of routing (for example, with modified time-to-live (TTL), MAC address, or QoS values) are duplicated (with the modifications) at the destination port.

  Features that can cause a packet to be dropped during transmit processing also affect the duplicated copy for SPAN. These features include IP standard and extended output ACLs and egress QoS policing.

- Both—In a SPAN session, you can also monitor a port or VLAN for both received and sent packets. This is the default.

Device congestion can cause packets to be dropped at ingress source ports, egress source ports, or SPAN destination ports. In general, these characteristics are independent of one another. For example:

- A packet might be forwarded normally but dropped from monitoring due to an oversubscribed SPAN destination port.

- An ingress packet might be dropped from normal forwarding, but still appear on the SPAN destination port.

- An egress packet dropped because of device congestion is also dropped from egress SPAN.

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 Rx monitor on port A and Tx monitor on port B. If a packet enters the device through port A and is switched to port B, both incoming and outgoing packets are sent to the destination port. Both packets are the same unless a Layer 3 rewrite occurs, in which case the packets are different because of the packet modification.

Source Ports

A source port (also called a monitored port) is a switched or routed port that you monitor for network traffic analysis.

The device supports any number of source ports (up to the maximum number of available ports on the device) and any number of source VLANs (up to the maximum number of VLANs supported).

However, the device supports a maximum of four sessions with source ports or VLANs. You cannot mix ports and VLANs in a single session.

A source port has these characteristics:

- It can be monitored in multiple SPAN sessions.

- Each source port can be configured with a direction (ingress, egress, or both) to monitor.

- It can be any port type (for example, EtherChannel, Gigabit Ethernet, and so forth).

- For EtherChannel sources, you can monitor traffic for the entire EtherChannel or individually on a physical port as it participates in the port channel.

- It can be an access port, trunk port, routed port, or voice VLAN port.

- It cannot be a destination port.

- Source ports can be in the same or different VLANs.

- You can monitor multiple source ports in a single session.

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 or VLANs and sends the SPAN packets to the user, usually a network analyzer.

A destination port has these characteristics:

- When a port is configured as a SPAN destination port, the configuration overwrites the original port configuration. When the SPAN destination configuration is removed, the port reverts to its previous configuration. If a configuration change is made to the port while it is acting as a SPAN destination port, the change does not take effect until the SPAN destination configuration had been removed.

- If the port was in an EtherChannel group, it is removed from the group while it is a destination port. If it was a routed port, it is no longer a routed port.

- It can be any Ethernet physical port.

- It cannot be a secure port.

- It cannot be a source port.

- It 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).

- When it is active, incoming traffic is disabled. The port does not transmit any traffic except that required for the SPAN session. Incoming traffic is never learned or forwarded on a destination port.

- If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.

- 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.

Local SPAN destination ports function differently with VLAN tagging and encapsulation:

- For local SPAN, if the **encapsulation replicate** keywords are specified for the destination port, these packets appear with the original encapsulation (untagged or IEEE 802.1Q). If these keywords are not specified, packets appear in the untagged format. Therefore, the output of a local SPAN session with **encapsulation replicate** enabled can contain a mixture of untagged or IEEE 802.1Q-tagged packets.

SPAN Interaction with Other Features

SPAN interacts with these features:

- STP—A destination port does not participate in STP while its SPAN or RSPAN session is active. The destination port can participate in STP after the SPAN or RSPAN session is disabled. On a source port, SPAN does not affect the STP status. STP can be active on trunk ports carrying an RSPAN VLAN.

- 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 remove the SPAN destination configuration. Changes in VLAN membership or trunk settings for a source port immediately take effect, and the respective SPAN sessions automatically adjust 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 physical 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.

  A physical port that belongs to an EtherChannel group can be configured as a SPAN source port and still be a part of the EtherChannel. In this case, data from the physical port is monitored as it participates in the EtherChannel. However, if a physical port that belongs to an EtherChannel group is configured as a SPAN destination, 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 inactive or suspended 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.

- 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.

- A secure port cannot be a SPAN destination port.

  For SPAN sessions, do not enable port security on ports with monitored egress when ingress forwarding is enabled on the destination port.

- An IEEE 802.1x port can be a SPAN source port. You can enable IEEE 802.1x on a port that is a SPAN destination port; however, IEEE 802.1x is disabled until the port is removed as a SPAN destination.

  For SPAN sessions, do not enable IEEE 802.1x on ports with monitored egress when ingress forwarding is enabled on the destination port.

Default SPAN Configuration

Table 1: Default SPAN Configuration

Feature	Default Setting
SPAN state	Disabled.

Feature	Default Setting
Source port traffic to monitor	Both received and sent traffic (**both**).
Encapsulation type (destination port)	Native form (untagged packets).
Ingress forwarding (destination port)	Disabled.

Configuration Guidelines

SPAN 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 SPAN

Creating a Local SPAN Session

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no monitor session** *session_number*
4. **monitor session** *session_number* **source** {**interface** *interface-id*} [**,** | **-**] [**both** | **rx** | **tx**]
5. **monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] }
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**enable** **Example:** `Device> ` **`enable`**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	**Purpose**
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 gigabitethernet0/1`
					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.
					
					• (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 gigabitethernet0/2`	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.

	Command or Action	Purpose
		• 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.
Step 6	**end** **Example:** Device(config)# **end**	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** Device# **show running-config**	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** Device# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Creating a Local SPAN 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).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no monitor session** *session_number*
4. **monitor session** *session_number* **source** {**interface** *interface-id*} [**,** | **-**] [**both** | **rx** | **tx**]
5. **monitor session** *session_number* **destination** {**interface** *interface-id* [**encapsulation replicate ingress** {**vlan** *vlan-id*} | **ingress** {**vlan** *vlan-id*}]}
6. **end**

7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	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 gigabitethernet0/1 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: Device(config)# **monitor session 2 destination interface gigabitethernet0/2 ingress vlan 6**	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. • 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.

	Command or Action	Purpose
Step 6	**end** **Example:** Device(config)# **end**	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** Device# **show running-config**	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** Device# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Monitoring SPAN 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 Enter the **all** keyword to sh the **local** keyword to show and the **range** keyword to s sessions.

SPAN Configuration Examples

Example: Configuring Local SPAN

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 gigabitethernet0/1
```

```
Device(config)# monitor session 1 destination interface gigabitethernet0/2
encapsulation replicate
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 gigabitethernet0/1
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 gigabitethernet0/1 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 gigabitethernet0/2
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 gigabitethernet0/1 rx
Device(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation
replicate ingress vlan 6
Device(config)# end
```

Examples: Creating an RSPAN VLAN

This example shows how to create the RSPAN VLAN 901:

```
Device> enable
Device# configure terminal
Device(config)# vlan 901
Device(config-vlan)# remote span
Device(config-vlan)# end
```

This example shows how to remove any existing RSPAN configuration for session 1, configure RSPAN session 1 to monitor multiple source interfaces, and configure the destination as RSPAN VLAN 901:

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1
Device(config)# monitor session 1 source interface gigabitethernet1/0/1 tx
Device(config)# monitor session 1 source interface gigabitethernet1/0/2 rx
Device(config)# monitor session 1 source interface port-channel 2
Device(config)# monitor session 1 destination remote vlan 901
Device(config)# end
```

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

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Device(config)# monitor session 2 filter vlan 1 - 5 , 9
Device(config)# monitor session 2 destination remote vlan 902
Device(config)# end
```

This example shows how to configure VLAN 901 as the source remote VLAN and port 1 as the destination interface:

```
Device> enable
Device# configure terminal
Device(config)# monitor session 1 source remote vlan 901
Device(config)# monitor session 1 destination interface gigabitethernet2/0/1
Device(config)# end
```

This example shows how to configure VLAN 901 as the source remote VLAN in RSPAN session 2, to configure Gigabit Ethernet source port 2 as the destination interface, and to enable forwarding of incoming traffic on the interface with VLAN 6 as the default receiving VLAN:

```
Device> enable
Device# configure terminal
Device(config)# monitor session 2 source remote vlan 901
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress vlan 6
Device(config)# end
```

Feature History and Information for SPAN

Release	Modification
Cisco IOS 15.0(2)EXCisco IOS 15.2(5)E	Switch Port Analyzer (SPAN): Allows monitoring of device traffic on a port or VLAN using a sniffer/analyzer or RMON probe. This feature was introduced.

Release	Modification
Cisco IOS 15.0(2)EXCisco IOS 15.2(5)E	SPAN destination port support on EtherChannels: Provides the ability to configure a SPAN destination port on an EtherChannel. This feature was introduced.
Cisco IOS 15.0(2)EXCisco IOS 15.2(5)E	Switch Port Analyzer (SPAN) - distributed egress SPAN: Provides distributed egress SPAN functionality onto line cards in conjunction with ingress SPAN already been distributed to line cards. By distributing egress SPAN functionalities onto line cards, the performance of the system is improved. This feature was introduced.
Cisco IOS Release 15.2(6)E2	Support for 4 SPAN sessions was introduced.