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 http://www.cisco.com/go/cfn. 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 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 | all}` 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 switch supports only one local SPAN session.

• SPAN sessions do not interfere with the normal operation of the switch. 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 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.

### Default SPAN Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPAN state</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Source port traffic to monitor</td>
<td>Both received and sent traffic (both).</td>
</tr>
<tr>
<td>Encapsulation type (destination port)</td>
<td>Native form (untagged packets).</td>
</tr>
</tbody>
</table>
Feature | Default Setting
--- | ---
Ingress forwarding (destination port) | Disabled.

## Configuration Guidelines

### SPAN Configuration Guidelines

- To remove a source or destination port or VLAN from the SPAN session, use the `no monitor session session_number source {interface interface-id | vlan vlan-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.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable` | Enables privileged EXEC mode.  
**Example:**  
```bash  
Switch> enable  
``` |
| Step 2 | `configure terminal` | Enters global configuration mode.  
**Example:**  
```bash  
Switch# configure terminal  
``` |
| Step 3 | `no monitor session session_number` | Removes existing SPAN configuration for the specified session. The range is 1 to 4.  
**Example:**  
```bash  
Switch(config)# no monitor session 1  
``` |
| Step 4 | `monitor session session_number source {interface interface-id} [., -] [both | rx | tx]` | Specifies the SPAN session and the source port (monitored port).  
**Example:**  
```bash  
```  
- For `session_number`, the range is 1 to 4.
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `Switch(config)# monitor session 1 source interface gigabitethernet0/1` | • For `interface-id`, specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (port-channel `port-channel-number`). 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:**

`Switch(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.

• 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
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).

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | enable            | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| 2    | configure terminal| Enters global configuration mode. |
| 6    | end               | Returns to privileged EXEC mode.  
  Example:  
  Switch(config)# end |
| 7    | show running-config | Verifies your entries.  
  Example:  
  Switch# show running-config |
| 8    | copy running-config startup-config | (Optional) Saves your entries in the configuration file.  
  Example:  
  Switch# copy running-config startup-config |

**Note**

You can use `monitor session session_number destination` command multiple times to configure multiple destination ports.

You must enter a space before and after the hyphen when using the comma.
### Configuring SPAN

#### Creating a Local SPAN Session and Configuring Incoming Traffic

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 3    | no monitor session \{session_number | all | local | remote\} | Removes any existing SPAN configuration for the session.  
- For session_number, the range is 1 to 66.  
- all—Removes all SPAN sessions.  
- local—Removes all local sessions.  
- remote—Removes all remote SPAN sessions. |
|      | Example: | |
|      | Switch(config)# no monitor session all | |
| 4    | monitor session session_number source \{interface interface-id | vlan vlan-id\} [, | -] [both | rx | tx] | Specifies the SPAN session and the source port (monitored port). |
|      | Example: | |
|      | Switch(config)# monitor session 2 source gigabitethernet1/0/1 rx | |
| 5    | monitor session session_number destination \{interface interface-id [, | -] [encapsulation replicate]ingress \{dot1q vlan vlan-id | untagged vlan vlan-id | vlan vlan-id\}\} | 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) [, | -]—Specifies a series or range of interfaces. Enter a space before and after the comma or hyphen.  
- ingress enables forwarding of incoming traffic on the destination port and to specify the encapsulation type:  
  - dot1q vlan vlan-id—Accepts incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.  
  - untagged vlan vlan-id or vlan vlan-id—Accepts incoming packets with untagged encapsulation type with the specified VLAN as the default VLAN. |
|      | Example: | |
|      | Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress dot1q vlan 6 | |
### 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show monitor session</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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.

```bash
Switch> enable
```
Switch# configure terminal
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet0/1
Switch(config)# monitor session 1 destination interface gigabitethernet0/2
enapsulation replicate
Switch(config)# end

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

Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 1 source interface gigabitethernet0/1
Switch(config)# end

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

Switch> enable
Switch# configure terminal
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.

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.

Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 destination interface gigabitethernet0/2
Switch(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:

Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source gigabitethernet0/1 rx
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation replicate ingress vlan 6
Switch(config)# end

---

**Additional References**

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Commands</td>
<td></td>
</tr>
</tbody>
</table>
### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

### Feature History and Information for SPAN

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(5)E Cisco IOS 15.2(5)E</td>
<td>Switch Port Analyzer (SPAN): Allows monitoring of switch traffic on a port or VLAN using a sniffer/analyzer or RMON probe. This feature was introduced.</td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>SPAN destination port support on EtherChannels: Provides the ability to configure a SPAN destination port on an EtherChannel. This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>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.</td>
</tr>
</tbody>
</table>