



## Configuring SPAN and RSPAN

---

This chapter describes how to configure Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) on your Catalyst 2950 or Catalyst 2955 switch.



### Note

---

For complete syntax and usage information for the commands used in this chapter, refer to the command reference for this release.

---

This chapter consists of these sections:

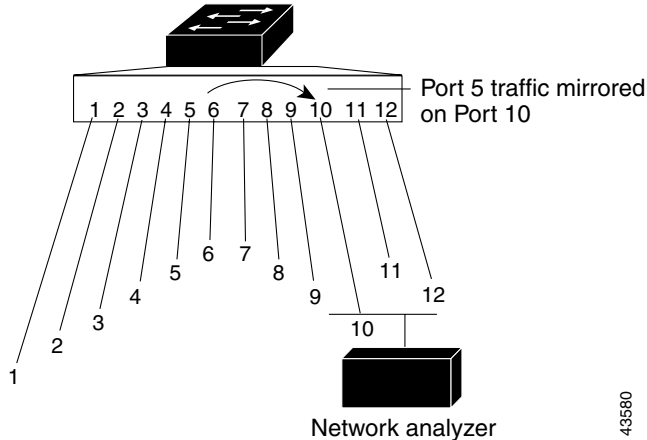
- [Understanding SPAN and RSPAN, page 25-1](#)
- [Configuring SPAN, page 25-7](#)
- [Configuring RSPAN, page 25-12](#)
- [Displaying SPAN and RSPAN Status, page 25-17](#)

## Understanding SPAN and RSPAN

You can analyze network traffic passing through ports 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 or security device. SPAN mirrors received or transmitted (or both) traffic on one or more source ports to a destination port for analysis.

For example, in [Figure 25-1](#), 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.

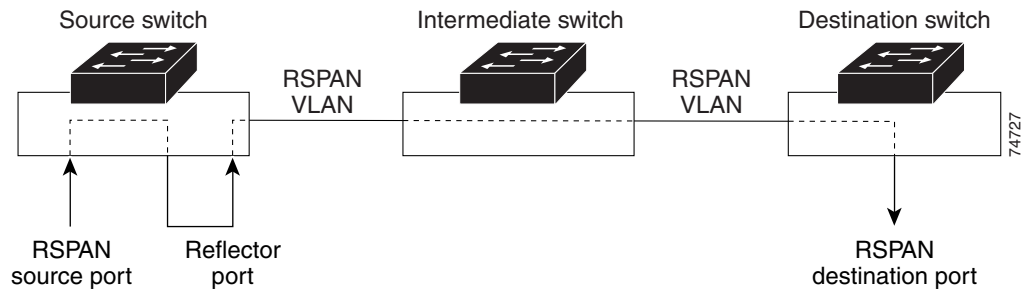
Figure 25-1 Example SPAN Configuration



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

RSPAN extends SPAN by enabling remote monitoring of multiple switches across your network. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The SPAN traffic from the sources is copied onto the RSPAN VLAN through a reflector port and then forwarded over trunk ports that are carrying the RSPAN VLAN to any RSPAN destination session monitoring the RSPAN VLAN, as shown in Figure 25-2.

Figure 25-2 Example of RSPAN Configuration



SPAN and RSPAN do 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. Except for traffic that is required for the SPAN or RSPAN session, reflector ports and 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.

**Note**

You cannot use the RSPAN destination port to inject traffic from a network security device. The switch does not support ingress forwarding on an RSPAN destination port.

## SPAN and RSPAN Concepts and Terminology

This section describes concepts and terminology associated with SPAN and RSPAN configuration.

### SPAN Session

A local 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.

An RSPAN session is an association of source ports across your network with an RSPAN VLAN. The destination source is the RSPAN VLAN.

SPAN sessions do not interfere with the normal operation of the switch. However, an oversubscribed SPAN destination, for example, a 10-Mbps port monitoring a 100-Mbps port, results in dropped or lost packets.

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. 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, if tagging is enabled, the packets appear with the 802.1Q header. If no tagging is specified, packets appear in the native format.

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.

- 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.

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, you can monitor a series or range of ports 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 local SPAN session or RSPAN source 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.

## 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 port.

The destination port has these characteristics:

- It must reside on the same switch as the source port (for a local SPAN session).
- It can be any Ethernet physical port.
- It cannot be a source port or a reflector port.
- It cannot be an EtherChannel group or a VLAN.
- It can be a physical port that is assigned to an EtherChannel group, even if the EtherChannel group has been specified as a SPAN source. The port is removed from the group while it is configured as a SPAN destination port.
- The port does not transmit any traffic except that required for the SPAN session.
- If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.
- It does not participate in spanning tree while the SPAN session is active.
- When it is a destination port, it does not participate in any of the Layer 2 protocols (STP, VTP, CDP, DTP, PagP, or LACP).
- No address learning occurs on the destination port.
- A destination port receives copies of sent and received traffic for all monitored source ports. If a destination port is oversubscribed, it could become congested. This could affect traffic forwarding on one or more of the source ports.

## Reflector Port

The reflector port is the mechanism that copies packets onto an RSPAN VLAN. The reflector port forwards only the traffic from the RSPAN source session with which it is affiliated. Any device connected to a port set as a reflector port loses connectivity until the RSPAN source session is disabled.

The reflector port has these characteristics:

- It is a port set to loopback.
- It cannot be an EtherChannel group, it does not trunk, and it cannot do protocol filtering.
- It can be a physical port that is assigned to an EtherChannel group, even if the EtherChannel group is specified as a SPAN source. The port is removed from the group while it is configured as a reflector port.
- A port used as a reflector port cannot be a SPAN source or destination port, nor can a port be a reflector port for more than one session at a time.
- It is invisible to all VLANs.
- The native VLAN for looped-back traffic on a reflector port is the RSPAN VLAN.
- The reflector port loops back untagged traffic to the switch. The traffic is then placed on the RSPAN VLAN and flooded to any trunk ports that carry the RSPAN VLAN.
- Spanning tree is automatically disabled on a reflector port.
- A reflector port receives copies of sent and received traffic for all monitored source ports. If a reflector port is oversubscribed, it could become congested. This could affect traffic forwarding on one or more of the source ports.

If the bandwidth of the reflector port is not sufficient for the traffic volume from the corresponding source ports, the excess packets are dropped. A 10/100 port reflects at 100 Mbps. A Gigabit port reflects at 1 Gbps.

## SPAN Traffic

You can use local SPAN to monitor all network traffic, including multicast and bridge protocol data unit (BPDU) packets, and Cisco Discovery Protocol (CDP), VLAN Trunk Protocol (VTP), Dynamic Trunking Protocol (DTP), Spanning Tree Protocol (STP), Port Aggregation Protocol (PagP), and Link Aggregation Control Protocol (LACP) packets. You cannot use RSPAN to monitor Layer 2 protocols. See the [“RSPAN Configuration Guidelines” section on page 25-12](#) for more information.

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 sources a1 Rx monitor and the a2 Rx and Tx monitor to 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.

## SPAN and RSPAN Interaction with Other Features

SPAN interacts with these features:

- Spanning Tree Protocol (STP)—A destination port or a reflector port does not participate in STP while its SPAN or RSPAN session is active. The destination or reflector 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.
- 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 Trunking Protocol (VTP)—You can use VTP to prune an RSPAN VLAN between switches.
- VLAN and trunking—You can modify VLAN membership or trunk settings for source, destination, or reflector ports at any time. However, changes in VLAN membership or trunk settings for a destination or reflector port do not take effect until you disable the SPAN or RSPAN session. Changes in VLAN membership or trunk settings for a source port immediately take effect, and the SPAN session automatically adjusts 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 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, destination, or reflector port, 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 *down* or *standalone* state.

If a physical port that belongs to an EtherChannel group is a destination or reflector port and the EtherChannel group is a source, the port is removed from the EtherChannel group and from the list of monitored ports.

- 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.
- Port security—A secure port cannot be a SPAN destination port.

## SPAN and RSPAN Session Limits

You can configure (and store in NVRAM) one local SPAN session or multiple RSPAN sessions on a switch. The number of active sessions and combinations are subject to these restrictions:

- SPAN or RSPAN source (rx, tx, both): 1 active session limit. (SPAN and RSPAN are mutually exclusive on a source switch).
- RSPAN source sessions have one destination per session with an RSPAN VLAN associated for that session.
- Each RSPAN destination session has one or more destination interfaces for each RSPAN VLAN that they support.
- RSPAN destination sessions are limited to two, or one if a local SPAN or a source RSPAN session is configured on the same switch.

## Default SPAN and RSPAN Configuration

Table 25-1 shows the default SPAN and RSPAN configuration.

**Table 25-1 Default SPAN and RSPAN Configuration**

Feature	Default Setting
SPAN state	Disabled.
Source port traffic to monitor	Both received and sent traffic ( <b>both</b> ).
Encapsulation type (destination port)	Native form (no encapsulation type header).
Ingress forwarding (destination port)	Disabled.

## Configuring SPAN

This section describes how to configure SPAN on your switch. It contains this configuration information:

- [SPAN Configuration Guidelines, page 25-8](#)
- [Creating a SPAN Session and Specifying Ports to Monitor, page 25-8](#)
- [Creating a SPAN Session and Enabling Ingress Traffic, page 25-10](#)
- [Removing Ports from a SPAN Session, page 25-11](#)

## SPAN Configuration Guidelines

Follow these guidelines when configuring SPAN:

- SPAN sessions can coexist with RSPAN sessions within the limits described in the “[SPAN and RSPAN Session Limits](#)” section on page 25-7.
- 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 SPAN source ports, you can monitor sent 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.
- 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.
- 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 the 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	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>no monitor session</b> { <i>session_number</i>   <b>all</b>   <b>local</b>   <b>remote</b> }	Clear any existing SPAN configuration for the session. For <i>session_number</i> , specify 1. Specify <b>all</b> to remove all SPAN sessions, <b>local</b> to remove all local sessions, or <b>remote</b> to remove all remote SPAN sessions.

	Command	Purpose
Step 3	<b>monitor session</b> <i>session_number</i> <b>source interface</b> <i>interface-id</i> [,   -] [ <b>both</b>   <b>rx</b>   <b>tx</b> ]	<p>Specify the SPAN session and the source port (monitored port).</p> <p>For <i>session_number</i>, specify 1.</p> <p>For <i>interface-id</i>, specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (<b>port-channel</b> <i>port-channel-number</i>).</p> <p>(Optional) [,   -] Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.</p> <p>(Optional) Specify the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic.</p> <ul style="list-style-type: none"> <li>• <b>both</b>—Monitor both received and sent traffic.</li> <li>• <b>rx</b>—Monitor received traffic.</li> <li>• <b>tx</b>—Monitor sent traffic.</li> </ul>
Step 4	<b>monitor session</b> <i>session_number</i> <b>destination interface</b> <i>interface-id</i> [ <b>encapsulation</b> { <b>dot1q</b> }]	<p>Specify the SPAN session and the destination port (monitoring port).</p> <p>For <i>session_number</i>, specify 1.</p> <p>For <i>interface-id</i>, specify the destination port. Valid interfaces include physical interfaces.</p> <p>(Optional) Specify the encapsulation header for outgoing packets. If not specified, packets are sent in native form.</p> <ul style="list-style-type: none"> <li>• <b>dot1q</b>—Use 802.1Q encapsulation.</li> </ul>
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show monitor</b> [ <b>session</b> <i>session_number</i> ]	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

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 10.

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface fastethernet0/1
Switch(config)# monitor session 1 destination interface fastethernet0/10
encapsulation dot1q
Switch(config)# end
```

## Creating a SPAN Session and Enabling Ingress Traffic

Beginning in privileged EXEC mode, follow these steps to create a SPAN session, to specify the source and destination ports, and to enable ingress traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance):

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>no monitor session</b> { <i>session_number</i>   <b>all</b>   <b>local</b>   <b>remote</b> }	Clear any existing SPAN configuration for the session. For <i>session_number</i> , specify 1. Specify <b>all</b> to remove all SPAN sessions, <b>local</b> to remove all local sessions, or <b>remote</b> to remove all remote SPAN sessions.
Step 3	<b>monitor session</b> <i>session_number</i> <b>source interface</b> <i>interface-id</i> [,   -] [ <b>both</b>   <b>rx</b>   <b>tx</b> ]	Specify the SPAN session and the source port (monitored port). For <i>session_number</i> , specify 1. For <i>interface-id</i> , specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces ( <b>port-channel</b> <i>port-channel-number</i> ). (Optional) [,   -] Specify a series or range of interfaces. Enter a space before and 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 sent and received traffic. <ul style="list-style-type: none"> <li>• <b>both</b>—Monitor both received and sent traffic.</li> <li>• <b>rx</b>—Monitor received traffic.</li> <li>• <b>tx</b>—Monitor sent traffic.</li> </ul>
Step 4	<b>monitor session</b> <i>session_number</i> <b>destination interface</b> <i>interface-id</i> [ <b>encapsulation</b> { <b>dot1q</b> }] [ <b>ingress vlan</b> <i>vlan id</i> ]	Specify the SPAN session, the destination port (monitoring port), the packet encapsulation, and the ingress VLAN. For <i>session_number</i> , specify 1. For <i>interface-id</i> , specify the destination port. Valid interfaces include physical interfaces. (Optional) Specify the encapsulation header for outgoing packets. If not specified, packets are sent in native form. <ul style="list-style-type: none"> <li>• <b>dot1q</b>—Use 802.1Q encapsulation.</li> </ul> (Optional) Enter <b>ingress vlan</b> <i>vlan id</i> to enable ingress forwarding and specify a default VLAN.
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show monitor</b> [ <b>session</b> <i>session_number</i> ]	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that does not support 802.1Q encapsulation.

```
Switch(config)# monitor session 1 destination interface Fa 0/5 ingress vlan 5
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that supports 802.1Q encapsulation.

```
Switch(config)# monitor session 1 destination interface Fa 0/5 encapsulation dot1q ingress
vlan 5
```

This example shows how to disable ingress traffic forwarding on the destination port.

```
Switch(config)# monitor session 1 destination interface Fa 0/5 encapsulation dot1q
```

## 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	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>no monitor session</b> <i>session_number</i> <b>source interface</b> <i>interface-id</i> [,   -] [ <b>both</b>   <b>rx</b>   <b>tx</b> ]	Specify the characteristics of the source port (monitored port) and SPAN session to remove.  For <i>session</i> , specify 1.  For <i>interface-id</i> , specify the source port to no longer monitor. Valid interfaces include physical interfaces and port-channel logical interfaces ( <b>port-channel</b> <i>port-channel-number</i> ).  (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 before and after the comma; enter a space before and after the hyphen.  (Optional) Specify the direction of traffic ( <b>both</b> , <b>rx</b> , or <b>tx</b> ) to no longer monitor. If you do not specify a traffic direction, both transmit and receive are disabled.
Step 3	<b>end</b>	Return to privileged EXEC mode.
Step 4	<b>show monitor</b> [ <b>session</b> <i>session_number</i> ]	Verify your entries.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

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. To change the encapsulation type back to the default (native), use the **monitor session** *session\_number* **destination interface** *interface-id* without the **encapsulation** keyword.

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

```
Switch(config)# no monitor session 1 source interface fastEthernet0/1
Switch(config)# end
```

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 fastEthernet0/1 rx
```

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

## Configuring RSPAN

This section describes how to configure RSPAN on your switch. It contains this configuration information:

- [RSPAN Configuration Guidelines, page 25-12](#)
- [Creating an RSPAN Session, page 25-13](#)
- [Creating an RSPAN Destination Session, page 25-15](#)
- [Removing Ports from an RSPAN Session, page 25-16](#)

## RSPAN Configuration Guidelines

To use the RSPAN feature described in this section, you must have the EI installed on your switch. Follow these guidelines when configuring RSPAN:

- All the items in the [“SPAN Configuration Guidelines” section on page 25-8](#) apply to RSPAN.



### Note

As RSPAN VLANs have special properties, you should reserve a few VLANs across your network for use as RSPAN VLANs; do not assign access ports to these VLANs.

- RSPAN sessions can coexist with SPAN sessions within the limits described in the [“SPAN and RSPAN Session Limits” section on page 25-7](#).
- If traffic for a port is monitored in one direction, you can use Catalyst 2950 or 2955 switches as source, intermediate, or destination switches.
- If traffic for a port is monitored in both directions, make sure that the intermediate switches and the destination switch are switches other than Catalyst 2950 or 2955 switches, such as Catalyst 3550, 3750, or 6000 switches.
- For RSPAN configuration, you can distribute the source ports and the destination ports across multiple switches in your network.
- A port cannot serve as an RSPAN source port or RSPAN destination port while designated as an RSPAN reflector port.
- When you configure a switch port as a reflector port, it is no longer a normal switch port; only looped-back traffic passes through the reflector port.
- RSPAN does not support BPDU packet monitoring or other Layer 2 switch protocols.
- In a network consisting of only Catalyst 2950 or Catalyst 2955 switches, you must use a unique RSPAN VLAN session on each source switch. If more than one source switch uses the same RSPAN VLAN, the switches are limited to act only as source switches to ensure the delivery of all monitored traffic to the destination switch.

- You can configure any VLAN as an RSPAN VLAN as long as these conditions are met:
  - The RSPAN VLAN is not configured as a native VLAN.
  - Extended range RSPAN VLANs will not be propagated to other switches using VTP.
  - No access port is configured in the RSPAN VLAN.
  - All participating switches support RSPAN.



**Note** The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 through 1005 (reserved to Token Ring and FDDI VLANs).

- You should create an RSPAN VLAN before configuring an RSPAN source or destination session.
- If you enable VTP and VTP pruning, RSPAN traffic is pruned in the trunks to prevent the unwanted flooding of RSPAN traffic across the network for VLAN-IDs that are lower than 1005.

## Creating an RSPAN Session

First create an RSPAN VLAN that *does not* exist for the RSPAN session in any of the switches that will participate in RSPAN. With VTP enabled in the network, you can create the RSPAN VLAN in one switch, and VTP propagates it to the other switches in the VTP domain for VLAN-IDs that are lower than 1005. See the “[Creating or Modifying an Ethernet VLAN](#)” section on page 17-8 for more information about creating an RSPAN VLAN.

Use VTP pruning to get efficient flow of RSPAN traffic, or manually delete the RSPAN VLAN from all trunks that do not need to carry the RSPAN traffic.

After creating the RSPAN VLAN, begin in privileged EXEC mode, and follow these steps to start an RSPAN source session and to specify the source (monitored) ports and the destination RSPAN VLAN.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>no monitor session</b> { <i>session_number</i>   <b>all</b>   <b>local</b>   <b>remote</b> }	Clear any existing RSPAN configuration for the session. For <i>session_number</i> , specify the session number identified with this RSPAN session. Specify <b>all</b> to remove all RSPAN sessions, <b>local</b> to remove all local sessions, or <b>remote</b> to remove all remote SPAN sessions.

	Command	Purpose
Step 3	<b>monitor session</b> <i>session_number</i> <b>source interface</b> <i>interface-id</i> [,   -] [ <b>both</b>   <b>rx</b>   <b>tx</b> ]	<p>Specify the RSPAN session and the source port (monitored port).</p> <p>For <i>session_number</i>, specify the session number identified with this RSPAN session.</p> <p>For <i>interface-id</i>, specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (<b>port-channel</b> <i>port-channel-number</i>).</p> <p>(Optional) [,   -] Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.</p> <p>(Optional) Specify the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic.</p> <ul style="list-style-type: none"> <li>• <b>both</b>—Monitor both received and sent traffic.</li> <li>• <b>rx</b>—Monitor received traffic.</li> <li>• <b>tx</b>—Monitor sent traffic.</li> </ul>
Step 4	<b>monitor session</b> <i>session_number</i> <b>destination remote vlan</b> <i>vlan-id</i> <b>reflector-port</b> <i>interface</i>	<p>Specify the RSPAN session, the destination remote VLAN, and the reflector port.</p> <p>For <i>session_number</i>, enter the session number identified with this RSPAN session.</p> <p>For <i>vlan-id</i>, specify the RSPAN VLAN to carry the monitored traffic to the destination port. (See the “<a href="#">Creating or Modifying an Ethernet VLAN</a>” section on page 17-8 for more information about creating an RSPAN VLAN.)</p> <p>For <i>interface</i>, specify the interface that will flood the RSPAN traffic onto the RSPAN VLAN.</p>
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show monitor</b> [ <b>session</b> <i>session_number</i> ]	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

This example shows how to clear any existing RSPAN configuration for session 1, configure RSPAN session 1 to monitor multiple source interfaces, and configure the destination RSPAN VLAN and the reflector-port.

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface fastEthernet0/10 tx
Switch(config)# monitor session 1 source interface fastEthernet0/2 rx
Switch(config)# monitor session 1 source interface fastEthernet0/3 rx
Switch(config)# monitor session 1 source interface port-channel 102 rx
Switch(config)# monitor session 1 destination remote vlan 901 reflector-port
fastEthernet0/1
Switch(config)# end
```

## Creating an RSPAN Destination Session

Beginning in privileged EXEC mode, follow these steps to create an RSPAN destination session and to specify the source RSPAN VLAN and the destination port:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>monitor session</b> <i>session_number</i> <b>source remote vlan</b> <i>vlan-id</i>	Specify the RSPAN session and the source RSPAN VLAN. For <i>session_number</i> , specify the session number identified with this RSPAN session. For <i>vlan-id</i> , specify the source RSPAN VLAN to monitor.
Step 3	<b>monitor session</b> <i>session_number</i> <b>destination interface</b> <i>interface-id</i> <b>[encapsulation {dot1q}]</b>	Specify the RSPAN session and the destination interface. For <i>session_number</i> , specify the session number identified with this RSPAN session. For <i>interface-id</i> , specify the destination interface. (Optional) Specify the encapsulation header for outgoing packets. If not specified, packets are sent in native form. <ul style="list-style-type: none"> <li><b>dot1q</b>—Use 802.1Q encapsulation.</li> </ul>
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show monitor</b> [ <b>session</b> <i>session_number</i> ]	Verify your entries.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

This example shows how to configure VLAN 901 as the source remote VLAN and port 5 as the destination interface:

```
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface fastEthernet0/5
Switch(config)# end
```

## Removing Ports from an RSPAN Session

Beginning in privileged EXEC mode, follow these steps to remove a port as an RSPAN source for a session:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>no monitor session</b> <i>session_number</i> <b>source interface</b> <i>interface-id</i> [,   -] [ <b>both</b>   <b>rx</b>   <b>tx</b> ]	Specify the characteristics of the RSPAN source port (monitored port) to remove.  For <i>session_number</i> , specify the session number identified with this RSPAN session.  For <i>interface-id</i> , specify the source port to no longer monitor. Valid interfaces include physical interfaces and port-channel logical interfaces ( <b>port-channel</b> <i>port-channel-number</i> ).  (Optional) Use [,   -] to specify a series or range of interfaces if they were configured. Enter a space before and after the comma; enter a space before and after the hyphen.  (Optional) Specify the direction of traffic ( <b>both</b> , <b>rx</b> , or <b>tx</b> ) to no longer monitor. If you do not specify a traffic direction, both transmit and receive are disabled.
Step 3	<b>end</b>	Return to privileged EXEC mode.
Step 4	<b>show monitor</b> [ <b>session</b> <i>session_number</i> ]	Verify your entries.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

This example shows how to remove port 1 as an RSPAN source for RSPAN session 1:

```
Switch(config)# no monitor session 1 source interface fastEthernet0/1
Switch(config)# end
```

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 fastEthernet0/1 rx
```

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

## Displaying SPAN and RSPAN Status

To display the status of the current SPAN or RSPAN configuration, use the **show monitor** privileged EXEC command.

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

```
Switch# show monitor session 1
Session 1
-----
Type                : Local Session
Source Ports        :
  RX Only           : None
  TX Only           : None
  Both              : Fa0/4
Source VLANs        :
  RX Only           : None
  TX Only           : None
  Both              : None
Source RSPAN VLAN   : None
Destination Ports   : Fa0/5
  Encapsulation: DOT1Q
  Ingress: Enabled, default VLAN = 5
Reflector Port      : None
Filter VLANs        : None
Dest RSPAN VLAN     : None
```

