Configuring Local SPAN and RSPAN

This chapter describes how to configure local Switched Port Analyzer (SPAN) and remote SPAN (RSPAN) on the Catalyst 6500 series switches. The Catalyst 6500 series switches support RSPAN with Release 12.1(13)E and later releases.

This chapter consists of these sections:

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

Understanding How Local SPAN and RSPAN Work

These sections describe how local SPAN and RSPAN work:

Local SPAN and RSPAN Overview

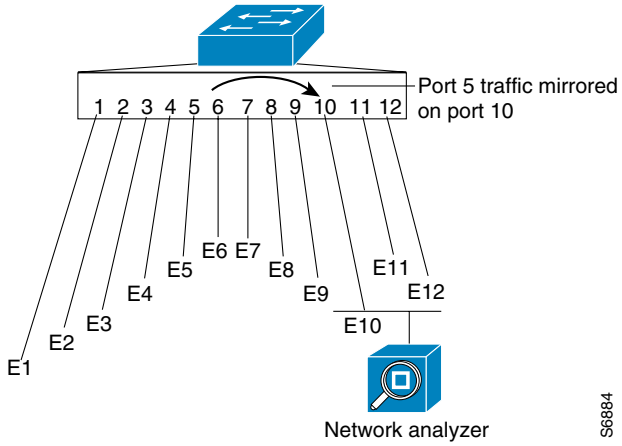
Local SPAN and RSPAN both select network traffic to send to a network analyzer such as a SwitchProbe device or other Remote Monitoring (RMON) probe. SPAN does not affect the switching of network traffic on source ports or VLANs. SPAN sends a copy of the packets received or transmitted by the source ports and VLANs to the destination port. You must dedicate the destination port for SPAN use.

These sections provide an overview of local SPAN and RSPAN:

Local SPAN Overview

Local SPAN supports source ports, source VLANs, and destination ports on the same Catalyst 6500 series switch. Local SPAN copies traffic from one or more source ports in any VLAN or from one or more VLANs to a destination port for analysis (see Figure 34-1). For example, as shown in Figure 34-1, all traffic on Ethernet port 5 (the source port) is copied to Ethernet port 10. A network analyzer on Ethernet port 10 receives all network traffic from Ethernet port 5 without being physically attached to Ethernet port 5.

Figure 34-1 Example SPAN Configuration



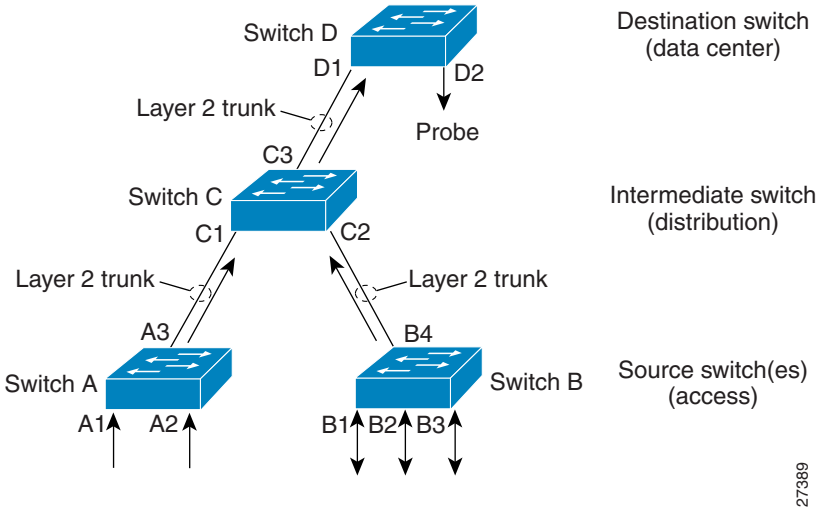
RSPAN Overview

RSPAN supports source ports, source VLANs, and destination ports on different switches, which provides remote monitoring of multiple switches across your network (see Figure 34-2). 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 RSPAN source ports can be trunks carrying the RSPAN VLAN. Local SPAN and RSPAN do not monitor the RSPAN traffic in the RSPAN VLAN seen on a source trunk.

The RSPAN traffic from the source ports or source VLANs is switched to the RSPAN VLAN and then forwarded to destination ports, which are in the RSPAN VLAN. The sources (ports or VLANs) in an RSPAN session can be different on different source switches but must be the same for all sources on each RSPAN source switch. Each RSPAN source switch must have either ports or VLANs as RSPAN sources.

Figure 34-2 RSPAN Configuration



Local SPAN and RSPAN Sessions

SPAN sessions (local or remote) allow you to monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports.

A local SPAN session is an association of a set of source ports and source VLANs with one or more destination ports. You configure a local SPAN session on a single network device. Local SPAN does not have separate source and destination sessions.

RSPAN consists of an RSPAN source session, an RSPAN VLAN, and an RSPAN destination session. You separately configure RSPAN source sessions and destination sessions on different network devices. To configure an RSPAN source session on one network device, you associate a set of source ports and VLANs with an RSPAN VLAN. To configure an RSPAN destination session on another device, you associate the destination port with the RSPAN VLAN.

Monitored Traffic

These sections describe the traffic that SPAN (local or remote) can monitor:

Monitored Traffic Direction

You can configure SPAN sessions to monitor ingress network traffic (called ingress SPAN), or to monitor egress network traffic (called egress SPAN), or to monitor traffic flowing in both directions.

Ingress SPAN copies network traffic received by the source ports and VLANs for analysis at the destination port. Egress SPAN copies network traffic transmitted from the source ports and VLANs. When you enter the **both** keyword, SPAN copies the network traffic received and transmitted by the source ports and VLANs to the destination port.

Monitored Traffic Type

By default, local SPAN monitors all network traffic, including multicast and bridge protocol data unit (BPDU) frames. RSPAN does not support BPDU monitoring.

Duplicate Traffic

In some configurations, SPAN sends multiple copies of the same source traffic to the destination port. For example, in a configuration with a bidirectional SPAN session (both ingress and egress) for two SPAN sources, called s1 and s2, to a SPAN destination port, called d1, if a packet enters the switch through s1 and is sent for egress from the switch to s2, ingress SPAN at s1 sends a copy of the packet to SPAN destination d1 and egress SPAN at s2 sends a copy of the packet to SPAN destination d1. If the packet was Layer 2 switched from s1 to s2, both SPAN packets would be the same. If the packet was Layer 3 switched from s1 to s2, the Layer-3 rewrite would alter the source and destination Layer 2 addresses, in which case the SPAN packets would be different.

SPAN Sources

These sections describe local SPAN and RSPAN sources:

Source Ports

A source port is a port monitored for network traffic analysis. You can configure both switched and routed ports as SPAN source ports. SPAN can monitor one or more source ports in a single SPAN session. You can configure source ports in any VLAN. Trunk ports can be configured as source ports and mixed with nontrunk source ports, but SPAN does not copy the encapsulation from a source trunk port.

Source VLANs

A source VLAN is a VLAN monitored for network traffic analysis. VLAN-based SPAN (VSPAN) uses a VLAN as the SPAN source. All the ports in the source VLANs become source ports.

Destination Ports

A destination port is a Layer 2 or Layer 3 LAN port to which SPAN sends traffic for analysis.

When you configure a port as a SPAN destination port, it can no longer receive any traffic. When you configure a port as a SPAN destination port, the port is dedicated for use only by the SPAN feature. A SPAN destination port does not forward any traffic except that required for the SPAN session.

With Release 12.1(13)E and later releases, you can configure trunk ports as destination ports, which allows destination trunk ports to transmit encapsulated traffic. With earlier releases, trunk ports stop trunking when you configure them as a destination port.

Local SPAN and RSPAN Configuration Guidelines and Restrictions

These sections describe local SPAN and RSPAN configuration guidelines and restrictions:

- Local SPAN and RSPAN Session Limits, page 34-5
- Local SPAN and RSPAN Source and Destination Limits, page 34-6
- Local SPAN and RSPAN Guidelines and Restrictions, page 34-6
- VSPAN Guidelines and Restrictions, page 34-7
- RSPAN Guidelines and Restrictions, page 34-7

Local SPAN and RSPAN Session Limits

These are the local SPAN and RSPAN session limits:

Total Sessions per Switch	Local SPAN Sessions	RSPAN Source Sessions	RSPAN Destination Sessions
66	2 (ingress or egress or both)	0	64
	1 ingress	1 (ingress or egress or both)	
	1 or 2 egress	0	

Local SPAN and RSPAN Source and Destination Limits

These are the local SPAN and RSPAN source and destination limits:

Sources and Destinations	Local SPAN Sessions	RSPAN Source Sessions	RSPAN Destination Sessions
Egress sources	1 (0 with a remote SPAN source session configured)	1 (0 with a local SPAN egress source session configured)	1 RSPAN VLAN
Ingress sources	64	64	
Destinations per session	64	1 RSPAN VLAN	64

Local SPAN and RSPAN Guidelines and Restrictions

These guidelines and restrictions apply to both local SPAN and RSPAN:

- Release 12.1(13)E and later releases support RSPAN.
- In releases earlier than 12.1(20)E, ports on the WS-X6548-GE-TX and WS-X6548V-GE-TX switching modules cannot be ingress SPAN sources when the switch is operating in truncated mode.
- You need a network analyzer to monitor destination ports.
- You can configure both Layer 2 LAN ports (LAN ports configured with the **switchport** command) and Layer 3 LAN ports (LAN ports not configured with the **switchport** command) as sources or destinations.
- With Release 12.1(13)E and later releases, you can configure destination ports as trunks to capture tagged traffic. With earlier releases, if you configure a trunk port as a destination port, SPAN suspends trunking on the port.
- A port specified as a destination port in one SPAN session cannot be a destination port for another SPAN session.
- A port configured as a destination port cannot be configured as a source port.
- A port channel interface (an EtherChannel) can be a source.
  - With Release 12.1(13)E and later releases, you cannot configure active member ports of an EtherChannel as source ports. Inactive member ports of an EtherChannel can be configured as sources but they are put into the suspended state and carry no traffic.
  - With releases earlier than 12.1(13)E, if you configure a member port of an EtherChannel as a SPAN source port, it is put into the suspended state and carries no traffic.
- A port channel interface (an EtherChannel) cannot be a destination.
  - With Release 12.1(13)E and later releases, you cannot configure active member ports of an EtherChannel as destination ports. Inactive member ports of an EtherChannel can be configured as destinations but they are put into the suspended state and carry no traffic.
  - With releases earlier than 12.1(13)E, if you configure a member port of an EtherChannel as a SPAN destination port, it is put into the suspended state and carries no traffic.
- You cannot mix individual source ports and source VLANs within a single session.
- If you specify multiple ingress source ports, the ports can belong to different VLANs.
- You cannot mix source VLANs and filter VLANs within a session. You can have source VLANs or filter VLANs, but not both at the same time.

- When enabled, local SPAN or RSPAN uses any previously entered configuration.
- When you specify sources and do not specify a traffic direction (ingress, egress, or both), “both” is used by default.
- You cannot configure destination ports to receive ingress traffic.
- Destination ports never participate in any spanning tree instance. Local SPAN includes BPDUs in the monitored traffic, so any BPDUs seen on the destination port are from the source port. RSPAN does not support BPDU monitoring.
- All packets sent through the switch for transmission from a port configured as an egress source are copied to the destination port, including packets that do not exit the switch through the port because STP has put the port into the blocking state, or on a trunk port because STP has put the VLAN into the blocking state on the trunk port.

VSPAN Guidelines and Restrictions

These are VSPAN guidelines and restrictions:

- For VSPAN sessions with both ingress and egress configured, two packets are forwarded from the destination port if the packets get switched on the same VLAN (one as ingress traffic from the ingress port and one as egress traffic from the egress port).
- VSPAN only monitors traffic that leaves or enters Layer 2 ports in the VLAN.
  - If you configure a VLAN as an ingress source and traffic gets routed into the monitored VLAN, the routed traffic is not monitored because it never appears as ingress traffic entering a Layer 2 port in the VLAN.
  - If you configure a VLAN as an egress source and traffic gets routed out of the monitored VLAN, the routed traffic is not monitored because it never appears as egress traffic leaving a Layer 2 port in the VLAN.

RSPAN Guidelines and Restrictions

These are RSPAN guidelines and restrictions:

- Any network device that supports RSPAN VLANs can be an RSPAN intermediate device.
- Networks impose no limit on the number of RSPAN VLANs that the networks carry.
- Intermediate switches might impose limits on the number of RSPAN VLANs that they can support.
- You must configure the RSPAN VLANs in all source, intermediate, and destination network devices. If enabled, the VLAN Trunking Protocol (VTP) can propagate configuration of VLANs numbered 1 through 1024 as RSPAN VLANs. You must manually configure VLANs numbered higher than 1024 as RSPAN VLANs on all source, intermediate, and destination network devices.
- 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.
- RSPAN VLANs can be used only for RSPAN traffic.
- Do not configure a VLAN used to carry management traffic as an RSPAN VLAN.
- Do not assign access ports to RSPAN VLANs. RSPAN puts access ports in an RSPAN VLAN into the suspended state.
- Do not configure any ports in an RSPAN VLAN except those selected to carry RSPAN traffic.

- MAC address learning is disabled on the RSPAN VLAN.
- You can use an output access control list (ACL) on the RSPAN VLAN in the RSPAN source switch to filter the traffic sent to an RSPAN destination.
- RSPAN does not support BPDU monitoring.
- Do not configure RSPAN VLANs as sources in VSPAN sessions.
- You can configure any VLAN as an RSPAN VLAN as long as all participating network devices support configuration of RSPAN VLANs and you use the same RSPAN VLAN for each RSPAN session in all participating network devices.
- Entering SPAN configuration commands does not clear previously configured SPAN parameters. You must enter the **no monitor session** command to clear configured SPAN parameters.

Configuring Local SPAN and RSPAN

These sections describe how to configure local SPAN and RSPAN:

Note With Release 12.1(11b)E and later releases, when you are in configuration mode you can enter EXEC mode-level commands by entering the **do** keyword before the EXEC mode-level command.

Local SPAN and RSPAN Configuration Overview

To configure a local SPAN session, use the same session number for the sources and the destination ports.

To configure an RSPAN source session, use the same session number for a source and a destination RSPAN VLAN.

To configure an RSPAN destination session, use the same session number for a source RSPAN VLAN and a destination port.

Configuring RSPAN VLANs

To configure a VLAN as an RSPAN VLAN, perform this task:

	Command	Purpose
Step 1	`Router(config)# vlan` *vlan_ID*`{[-`*vlan_ID*`]|[,`*vlan_ID*`])`	Creates or modifies an Ethernet VLAN, a range of Ethernet VLANs, or several Ethernet VLANs specified in a comma-separated list (do not enter space characters).
Step 2	`Router(config-vlan)# remote-span`	Configures the VLAN as an RSPAN VLAN.
	`Router(config-vlan)# no remote-span`	Clears the RSPAN VLAN configuration.
Step 3	`Router(config-vlan)# end`	Updates the VLAN database and returns to privileged EXEC mode.

Configuring Local or RSPAN Sources

Note To configure an RSPAN source session, configure a source with an RSPAN VLAN as the destination. To configure an RSPAN destination session, configure an RSPAN VLAN as the source and a port as the destination.

To configure a local SPAN or RSPAN source, perform this task:

Command	Purpose
`Router(config)# monitor session` *session_number* `source {{`*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list* | *single_vlan* | *vlan_list* | *vlan_range* | *mixed_vlan_list*`} [rx | tx | both]} | {remote vlan` *rspan_vlan_ID*`}}`	Configures the session number, the source ports, VLANs, or RSPAN VLAN, and the traffic direction to be monitored.
`Router(config)# no monitor session {`*session_number* `| all | local | range` *session_range*`[[,`*session_range*`],...] | remote}`	Clears the monitor configuration.

When configuring monitor sessions, note the following syntax information:

- *single_interface* is **interface** *type slot*/*port*; *type* is **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.
- *interface_list* is *single_interface* , *single_interface* , *single_interface* ...

  Note In lists, you must enter a space before and after the comma. In ranges, you must enter a space before and after the dash.

- *interface_range* is **interface** *type slot*/*first_port - last_port*
- *mixed_interface_list* is, in any order, *single_interface* , *interface_range* , ...
- *single_vlan* is a the ID number of a single VLAN.
- *vlan_list* is *single_vlan* , *single_vlan* , *single_vlan* ...

- *vlan_range* is *first_vlan_ID - last_vlan_ID*
- *mixed_vlan_list* is, in any order, *single_vlan* , *vlan_range* , ...

When clearing monitor sessions, note the following syntax information:

- The **no monitor session** *number* command entered with no other parameters clears session *session_number.*
- *session_range* is *first_session_number-last_session_number*

Note In the **no monitor session range** command, do not enter spaces before or after the dash. If you enter multiple ranges, do not enter spaces before or after the commas.

This example shows how to configure session 1 to monitor bidirectional traffic from Fast Ethernet port 5/1:

```
Router(config)# monitor session 1 source interface fastethernet 5/1
```

Monitoring Specific Source VLANs on a Source Trunk Port

To monitor specific VLANs when the local or RSPAN source is a trunk port, perform this task:

Command	Purpose
`Router(config)# monitor session` *session_number* `filter` {*vlan_ID*} [`,` | `-`]	Monitors specific VLANs when the source is a trunk port.
`Router(config)# no monitor session` *session_number* `filter` {*vlan_ID*}	Clears trunk source configuration.

This example shows how to monitor VLANs 1 through 5 and VLAN 9 when the source is a trunk port:

```
Router(config)# monitor session 2 filter vlan 1 - 5 , 9
```

Configuring Local SPAN and RSPAN Destinations

These sections describe how to configure local SPAN and RSPAN destinations:

- Configuring a Destination Port as an Unconditional Trunk, page 34-11
- Configuring a Local or RSPAN Destination, page 34-11

Configuring a Destination Port as an Unconditional Trunk

To tag the monitored traffic with Release 12.1(13)E and later releases, configure the destination port as a trunk.

To configure the destination port as a trunk, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface` *type*[1] *slot/port*	Selects the LAN port to configure.
Step 2	`Router(config-if)# switchport`	Configures the LAN port for Layer 2 switching (required only if the LAN port is not already configured for Layer 2 switching).
Step 3	`Router(config-if)# switchport trunk encapsulation {isl | dot1q}`	Configures the encapsulation, which configures the Layer 2 switching port as either an ISL or 802.1Q trunk.
Step 4	`Router(config-if)# switchport mode trunk`	Configures the port to trunk unconditionally.
Step 5	`Router(config-if)# switchport nonegotiate`	Configures the trunk not to use DTP.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to configure a port as an unconditional IEEE 802.1q trunk:

```
Router(config)# interface fastethernet 5/12
Router(config-if)# switchport
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# switchport mode trunk
Router(config-if)# switchport nonegotiate
```

Configuring a Local or RSPAN Destination

Note To configure an RSPAN source session, configure a source with an RSPAN VLAN as the destination. To configure an RSPAN destination session, configure an RSPAN VLAN as the source and a port as the destination.

To configure a local or RSPAN destination, perform this task:

Command	Purpose
`Router(config)# monitor session` *session_number* `destination` {*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list*} | {`remote vlan` *rspan_vlan_ID*}}	Configures the session number and the destination ports or RSPAN VLAN.
`Router(config)# no monitor session` {*session_number* | `all` | `local` | `range` *session_range*[[,*session_range*],...] | `remote`}	Clears the monitor configuration.

Note To tag the monitored traffic, you must configure the port to trunk unconditionally before you configure it as a destination (see the "Configuring a Destination Port as an Unconditional Trunk" section on page 34-11).

When configuring monitor sessions, note the following syntax information:

- *single_interface* is **interface** *type slot/port*; *type* is **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.
- *interface_list* is *single_interface* , *single_interface* , *single_interface* ...

Note In lists, you must enter a space before and after the comma. In ranges, you must enter a space before and after the dash.

- *interface_range* is **interface** *type slot/first_port - last_port*
- *mixed_interface_list* is, in any order, *single_interface* , *interface_range* , ...

When clearing monitor sessions, note the following syntax information:

- Enter the **no monitor session** *number* command with no other parameters to clear session *session_number.*
- *session_range* is *first_session_number-last_session_number*

Note In the **no monitor session range** command, do not enter spaces before or after the dash. If you enter multiple ranges, do not enter spaces before or after the commas.

This example shows how to configure Fast Ethernet port 5/48 as the destination for SPAN session 1:

```
Router(config)# monitor session 1 destination interface fastethernet 5/48
```

Verifying the Configuration

This example shows how to verify the configuration of session 2:

```
Router# show monitor session 2
Session 2
------------
Type : Remote Source Session

Source Ports:
    RX Only:       Fa3/1
Dest RSPAN VLAN:   901
Router#
```

This example shows how to display the full details of session 2:

```
Router# show monitor session 2 detail
Session 2
------------
Type : Remote Source Session

Source Ports:
    RX Only:       Fa1/1-3
    TX Only:       None
    Both:          None
Source VLANs:
    RX Only:       None
    TX Only:       None
    Both:          None
Source RSPAN VLAN: None
Destination Ports: None
Filter VLANs:      None
Dest RSPAN VLAN:   901
```

Configuration Examples

This example shows how to configure RSPAN source session 2:

```
Router(config)# monitor session 2 source interface fastethernet1/1 - 3 rx
Router(config)# monitor session 2 destination remote vlan 901
```

This example shows how to clear the configuration for sessions 1 and 2:

```
Router(config)# no monitor session range 1-2
```

This example shows how to configure an RSPAN source session with multiple sources:

```
Router(config)# monitor session 2 source interface fastethernet 5/15 , 7/3 rx
Router(config)# monitor session 2 source interface gigabitethernet 1/2 tx
Router(config)# monitor session 2 source interface port-channel 102
Router(config)# monitor session 2 source filter vlan 2 - 3
Router(config)# monitor session 2 destination remote vlan 901
```

This example shows how to remove sources for a session:

```
Router(config)# no monitor session 2 source interface fastethernet 5/15 , 7/3
```

This example shows how to remove options for sources for a session:

```
Router(config)# no monitor session 2 source interface gigabitethernet 1/2
Router(config)# no monitor session 2 source interface port-channel 102 tx
```

This example shows how to remove VLAN filtering for a session:

```
Router(config)# no monitor session 2 filter vlan 3
```

This example shows how to configure an RSPAN destination session:

```
Router(config)# monitor session 8 source remote vlan 901
Router(config)# monitor session 8 destination interface fastethernet 1/2 , 2/3
```