



Configuring SPAN and RSPAN

This chapter describes how to configure Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) on the Catalyst 6000 family switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6000 Family Command Reference* publication.

This chapter consists of these sections:

- SPAN and RSPAN Concepts and Terminology, page 32-1
- SPAN and RSPAN Session Limits, page 32-4
- Configuring SPAN, page 32-4
- Configuring RSPAN, page 32-8



Note

To configure SPAN or RSPAN from a Network Management Station (NMS), refer to the NMS documentation (see the “Using CiscoWorks2000” section on page 30-5).

SPAN and RSPAN Concepts and Terminology

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

SPAN Session

A SPAN session is an association of a destination port with a set of source ports, configured with parameters that specify the monitored network traffic. You can configure multiple SPAN sessions in a switched network. SPAN sessions do not interfere with the normal operation of the switches. You can enable or disable SPAN sessions with command-line interface (CLI) or SNMP commands. When enabled, a SPAN session might become active or inactive based on various events or actions, and this would be indicated by a syslog message. The “Status” field in the **show span** and **show rspan** commands displays the operational status of a SPAN or RSPAN session.

A SPAN or RSPAN destination session remains inactive after system power-up until the destination port is operational. An RSPAN source session remains inactive until any of the source ports are operational or the RSPAN VLAN becomes active.

Destination Port

A destination port (also called a *monitor port*) is a switch port where SPAN sends packets for analysis. Once a port becomes an active destination port, it does not forward any traffic except that required for the SPAN session. By default, an active destination port disables incoming traffic (from the network to the switching bus), unless you specifically enable the port. If incoming traffic is enabled for the destination port, it is switched in the native VLAN of the destination port. **The destination port does not participate in spanning tree while the SPAN session is active.** See the caution statement in the “Configuring SPAN from the CLI” section on page 32-6 for information on how to prevent loops in your network topology.

Only one destination port is allowed per SPAN session, and the same port cannot be a destination port for multiple SPAN sessions. A switch port configured as a destination port cannot be configured as a source port. EtherChannel ports cannot be SPAN destination ports.

If the trunking mode of a SPAN destination port is “on” or “nonegotiate” during SPAN session configuration, the SPAN packets forwarded by the destination port will have the encapsulation as specified by the trunk type; however, the destination port will stop trunking, and the **show trunk** command will reflect the trunking status for the port prior to SPAN session configuration.

Source Port

A source port is a switch port monitored for network traffic analysis. The traffic through the source ports can be categorized as ingress, egress, or both. You can monitor one or more source ports in a single SPAN session with user-specified traffic types (ingress, egress, or both) applicable for all the source ports.

You can configure source ports in any VLAN. You can configure VLANs as source ports (*src_vlans*), which means that all ports in the specified VLANs are source ports for the SPAN session.

Source ports are administrative (*Admin Source*) or operational (*Oper Source*) or both. Administrative source ports are the source ports or source VLANs specified during SPAN session configuration. Operational source ports are the source ports monitored by the destination port. For example, when source VLANs are used as the administrative source, the operational source is all the ports in all the specified VLANs.

The operational sources are always active ports. If a port is not in the spanning tree, it is not an operational source. All physical ports in an EtherChannel source are included in operational sources if the logical port is included in the spanning tree.

The destination port, if it belongs to any of the administrative source VLANs, is excluded from the operational source.

You can configure a port as a source port in multiple active SPAN sessions, but you cannot configure an active source port as a destination port for any SPAN session.

If a SPAN session is inactive, the “oper source” field will not be updated until the session becomes active.

Trunk ports can be configured as source ports, and can be mixed with nontrunk source ports; however, the encapsulation of the packets forwarded by the destination port are determined by the trunk settings of the destination port during SPAN session configuration.

Ingress SPAN

Ingress SPAN copies network traffic received by the source ports for analysis at the destination port.

Egress SPAN

Egress SPAN copies network traffic transmitted from the source ports for analysis at the destination port.

VSPAN

VLAN-based SPAN (VSPAN) is analysis of the network traffic in one or more VLANs. You can configure VSPAN as ingress SPAN, egress SPAN, or both. All the ports in the source VLANs become operational source ports for the VSPAN session. The destination port, if it belongs to any of the administrative source VLANs, is excluded from the operational source. If you add or remove ports from the administrative source VLANs, the operational sources are modified accordingly.

Use the following guidelines for VSPAN sessions:

- Trunk ports are included as source ports for VSPAN sessions, but only the VLANs that are in the Admin source list are monitored, provided these VLANs are active for the trunk.
- For VSPAN sessions with both ingress and egress SPAN configured, the system operates as follows based upon the type of supervisor engine you have:
 - WS-X6K-SUP1A-PFC, WS-X6K-SUP1A-MSFC, WS-X6K-SUP1A-MSFC2, WS-X6K-SUP2-PFC2, WS-X6K-SUP2-MSFC2—Two packets are forwarded by the SPAN destination port if the packets get switched on the same VLAN.
 - WS-X6K-SUP1-2GE, WS-X6K-SUP1A-2GE—Only one packet is forwarded by the SPAN destination port.
- An inband port is not included as Oper source for VSPAN sessions.
- When a VLAN is cleared, it is removed from the source list for VSPAN sessions.
- A VSPAN session is disabled if the Admin source VLANs list is empty.
- Inactive VLANs are not allowed for VSPAN configuration.
- A VSPAN session is made inactive if any of the source VLANs become RSPAN VLANs.

Trunk VLAN Filtering

Trunk VLAN filtering is analysis of network traffic on a selected set of VLANs on trunk source ports. You can combine trunk VLAN filtering with other source ports that belong to any of the selected VLANs, and you can also use trunk VLAN filtering for RSPAN. Based on the traffic type (ingress, egress, or both), SPAN sends a copy of the network traffic in the selected VLANs to the destination port.

Use trunk VLAN filtering only with trunk source ports. If you combine trunk VLAN filtering with other source ports that belong to VLANs not included in the selected list of filter VLANs, SPAN includes only the ports that belong to one or more of the selected VLANs in the operational sources.

When a VLAN is cleared, it is removed from the VLAN filter list. A SPAN session is disabled if the VLAN filter list becomes empty.

Trunk VLAN filtering is not applicable to VSPAN sessions.

SPAN Traffic

All network traffic, including the multicast and bridge protocol data unit (BPDU) packets, can be monitored using SPAN (RSPAN does not support monitoring of BPDU packets or Layer 2 protocol packets such as CDP, DTP, and VTP). Multicast packet monitoring is enabled by default.

In some SPAN configurations, multiple copies of the same source packet are sent to the SPAN destination port. For example, a bidirectional (both ingress and egress) SPAN session is configured for sources a1 and a2 to a destination port d1. If a packet enters the switch through a1 and gets switched to a2, both incoming and outgoing packets are sent to destination port d1; both packets would be the same (if a Layer-3 rewrite occurs, the packets are different). Similarly, for RSPAN sessions with sources distributed in multiple switches, the destination ports might forward multiple copies of the same packet.

SPAN and RSPAN Session Limits

You can configure (and store in NVRAM) a maximum of 30 SPAN sessions in a Catalyst 6000 family switch; the maximum is 5 SPAN sessions in a Catalyst 5000 family switch. See Table 32-1 for the supported combinations of SPAN/RSPAN sessions. You can configure multiple ports or VLANs as sources for each session.

Table 32-1 SPAN and RSPAN Session Limits

SPAN/RSPAN Sessions	Catalyst 5000 Family Switches ¹	Catalyst 6000 Family Switches ²
rx or both SPAN sessions	1	2
tx SPAN sessions	4	4
tx , rx , or both RSPAN source sessions	–	1
RSPAN destinations	–	24
Total SPAN sessions	5 ³	30 ⁴

1. RSPAN source is not supported in Catalyst 5000 family switches. RSPAN destination is shared with local egress sessions.
2. When an RSPAN source session is configured, it will reduce the limit for **rx** or **both** SPAN sessions by one.
3. 1 **rx** or **both** SPAN session + 4 **tx** SPAN sessions = 5 total SPAN sessions.
4. 2 **rx** or **both** SPAN sessions + 4 **tx** SPAN sessions + 24 RSPAN destination sessions = 30 total SPAN sessions.

Configuring SPAN

This section consists of the following:

- SPAN Hardware Requirements, page 32-5
- Understanding How SPAN Works, page 32-5
- SPAN Configuration Guidelines, page 32-5
- Configuring SPAN from the CLI, page 32-6

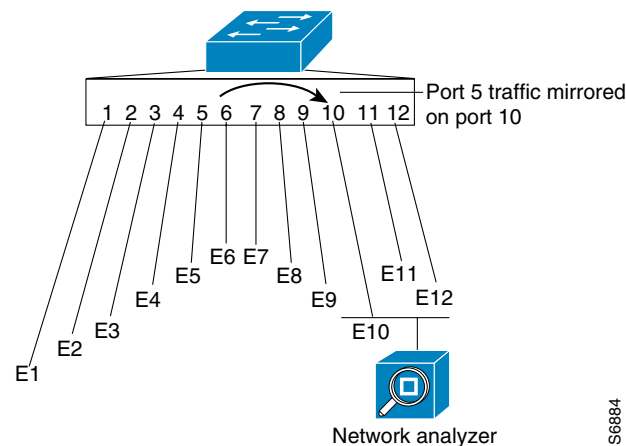
SPAN Hardware Requirements

All Catalyst 6000 family switch supervisor engines support the SPAN feature.

Understanding How SPAN Works

SPAN selects network traffic for analysis by a network analyzer such as a SwitchProbe device or other Remote Monitoring (RMON) probe. SPAN mirrors traffic from one or more source ports on any VLAN, from one or more VLANs, or from the sc0 console interface to a destination port for analysis (see Figure 32-1). In Figure 32-1, all traffic on Ethernet port 5 (the source port) is mirrored to Ethernet port 10. A network analyzer on Ethernet port 10 receives all network traffic from Ethernet port 5 without being physically attached to it.

Figure 32-1 SPAN Configuration



For SPAN configuration, the source ports and the destination port must be on the same switch.

SPAN does not affect the switching of network traffic on source ports; a copy of the packets received or transmitted by the source ports are sent to the destination port.

SPAN Configuration Guidelines

Follow these guidelines when configuring SPAN:

- Use a network analyzer to monitor ports.
- SPAN is not supported for ATM ports; it works with Ethernet 10/100/1000-Mbps ports.
- When enabled, SPAN uses any previously entered configuration; if you have not entered any configuration commands, SPAN uses default parameters.
- If you specify multiple SPAN source ports, the ports can belong to different VLANs.
- See “SPAN and RSPAN Session Limits” section on page 32-4.
- RSPAN sessions can coexist with SPAN sessions within the SPAN/RSPAN limits described in the “SPAN and RSPAN Session Limits” section on page 32-4.

- The **inpkts** option is disabled by default. Use the **inpkts** keyword with the **enable** option to allow the SPAN destination port to receive normal incoming traffic. Use the **disable** option to prevent the SPAN destination port from receiving normal incoming traffic.
- When you enable the **inpkts** option, a warning message notifies you that the destination port does not support the Spanning Tree Protocol (STP) and may cause loops if you enable this option.
- **Learning is enabled by default.** Use the **inpkts** keyword with the **learning** option to enable or disable learning for a specific port.
- You can specify a Multilayer Switch Module (MSM) port as the SPAN source port. However, you cannot specify an MSM port as the SPAN destination port.
- When you configure multiple SPAN sessions, the destination module number/port number must be known to index the particular SPAN session.

**Caution**

In software releases prior to software release 8.4(1), if you use the **set span** command without the **create** keyword, and you have only one session configured, the session is overwritten. If there are two SPAN sessions already configured, you receive an error message. If a matching destination port exists, the particular session is overwritten (with or without specifying the **create** keyword). If you specify the **create** keyword and there is no matching destination port, the session is created.

In software release 8.4(1) and later releases, the **create** keyword has been removed from the **set span** command. When you enable a SPAN session without the **create** keyword, and another session is available, the first session is not overwritten.

Configuring SPAN from the CLI

To configure SPAN, you specify the source, the destination port, the direction of the traffic through the source that you want to mirror to the destination port, and whether or not the destination port can receive packets.

To configure a SPAN port, perform this task in privileged mode:

	Task	Command
Step 1	Configure the SPAN source and destination ports.	set span { <i>src_mod/src_ports</i> <i>src_vlans</i> sc0 } { <i>dest_mod/dest_port</i> } [rx tx both] [inpkts { enable disable }] [learning { enable disable }] [multicast { enable disable }] [filter vlans...] [create]
Step 2	Verify the SPAN configuration.	show span

**Caution**

If the SPAN destination port is connected to another device and you enable reception of incoming packets (using the **inpkts enable** keywords), the SPAN destination port receives traffic for whatever VLAN the SPAN destination port belongs to. However, the SPAN destination port does *not* participate in spanning tree for that VLAN. Use caution when using the **inpkts** keyword to avoid creating network loops with the SPAN destination port or assigning the SPAN destination port to an unused VLAN.

This example shows how to configure SPAN so that both transmit and receive traffic from port 1/1 (the SPAN source) is mirrored on port 2/1 (the SPAN destination):

```
Console> (enable) set span 1/1 2/1

Destination      : Port 2/1
Admin Source     : Port 1/1
Oper Source      : Port 1/1
Direction        : transmit/receive
Incoming Packets: disabled
Learning         : enabled
Multicast        : enabled
Filter           : -
```

This example shows how to set VLAN 522 as the SPAN source and port 2/1 as the SPAN destination:

```
Console> (enable) set span 522 2/1

Destination      : Port 2/1
Admin Source     : VLAN 522
Oper Source      : Port 3/1-2
Direction        : transmit/receive
Incoming Packets: disabled
Learning         : enabled
Multicast        : enabled
Filter           : -
Console> (enable)
```

This example shows how to set VLAN 522 as the SPAN source and port 2/12 as the SPAN destination. Only transmit traffic is monitored. Normal incoming packets on the SPAN destination port are allowed.

```
Console> (enable) set span 522 2/12 tx inpkts enable

Destination      : Port 2/12
Admin Source     : VLAN 522
Oper Source      : Port 2/1-2
Direction        : transmit
Incoming Packets: enabled
Learning         : enabled
Multicast        : enabled
Filter           : -
Console> (enable)
```

This example shows how to set port 3/2 as the SPAN source and port 2/2 as the SPAN destination:

```
Console> (enable) set span 3/2 2/2 tx create

Destination      : Port 2/1
Admin Source     : port 3/1
Oper Source      : Port 3/1
Direction        : transmit/receive
Incoming Packets: disabled

Destination      : Port 2/2
Admin Source     : port 3/2
Oper Source      : Port 3/2
Direction        : transmit
Incoming Packets: disabled
Learning         : enabled
Multicast        : enabled
Filter           : -
Console> (enable)
```

To disable SPAN, perform this task in privileged mode:

Task	Command
Disable SPAN on the switch.	set span disable [<i>dest_mod/dest_port</i> <i>all</i>]

This example shows how to disable SPAN on the switch:

```
Console> (enable) set span disable 2/1
Disabled monitoring of VLAN 522 transmit traffic by Port 2/1
Console> (enable)
```

Configuring RSPAN

This section consists of the following:

- RSPAN Hardware Requirements, page 32-8
- Understanding How RSPAN Works, page 32-8
- RSPAN Configuration Guidelines, page 32-9
- Configuring RSPAN from the CLI, page 32-10
- RSPAN Configuration Examples, page 32-13

RSPAN Hardware Requirements

RSPAN supervisor engine requirements are as follows:

- For source switches—Catalyst 6000 family switch with supervisor engine WS-X6K-SUP1A-PFC or WS-X6K-SUP1A-MSFC.
- For destination or intermediate switches—Any Cisco switch supporting RSPAN VLAN.
- No third party or other Cisco switches can be placed in the end-to-end path for RSPAN traffic.

Understanding How RSPAN Works



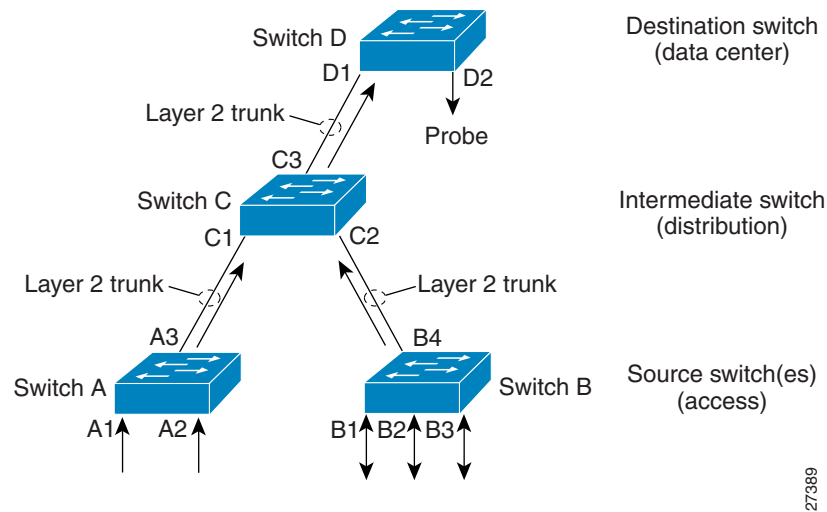
Note

See the “SPAN and RSPAN Concepts and Terminology” section on page 32-1 for concepts and terminology that apply to both SPAN and RSPAN configuration.

RSPAN has all the features of SPAN (see the “Understanding How SPAN Works” section on page 32-5), plus support for source ports and destination ports distributed across multiple switches, allowing remote monitoring of multiple switches across your network (see Figure 32-2).

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 SPAN traffic from the sources, which cannot be in the RSPAN VLAN, is switched to the RSPAN VLAN and then forwarded to destination ports configured in the RSPAN VLAN. The traffic type for sources (ingress, egress, or both) in an RSPAN session can be different in different source switches, but is the same for all sources in each source switch for each RSPAN session. Do not configure any ports in an RSPAN VLAN except those selected to carry RSPAN traffic. Learning is disabled on the RSPAN VLAN.

Figure 32-2 RSPAN Configuration



RSPAN Configuration Guidelines

Follow these guidelines when configuring RSPAN:



Tips

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



Tips

An output access control list (ACL) can be applied to RSPAN traffic to selectively filter specific flows. Specify these ACLs on the RSPAN VLAN in the RSPAN source switches.

- All the items in the “SPAN Configuration Guidelines” section on page 32-5 apply to RSPAN.
- RSPAN sessions can coexist with SPAN sessions within the SPAN/RSPAN limits described in the “SPAN and RSPAN Session Limits” section on page 32-4.
- For RSPAN configuration, the source ports and the destination port can be distributed across multiple switches.
- For RSPAN, trunking is required if you have a source switch with all source ports in one VLAN (VLAN 2 for example) and it is connected to the destination switch through an uplink port that is also in VLAN 2. With RSPAN, the traffic is forwarded to remote switches in the RSPAN VLAN. The RSPAN VLAN is configured only on trunk ports and not on access ports.
- The learning option applies to RSPAN destination ports only.
- RSPAN does not support monitoring of BPDU packets or Layer 2 protocol packets such as CDP, DTP, and VTP.
- To optimize bandwidth utilization in the connecting links, you can configure quality of service (QoS) parameters for the RSPAN VLAN in each of the participating source, intermediate, or destination switches.

27389

- Each Catalyst 6000 family switch can source a maximum of one RSPAN session (ingress, egress, or both). When you configure a remote ingress or bidirectional SPAN session in a source switch, the limit for local ingress or bidirectional SPAN sessions is reduced to one. There are no limits on the number of RSPAN sessions carried across the network within the RSPAN session limits (see “SPAN and RSPAN Session Limits” section on page 32-4).
- RSPAN VLANs cannot be included as sources for port-based RSPAN sessions when source trunk ports have active RSPAN VLANs. Additionally, RSPAN VLANs cannot be sources in VSPAN sessions.
- You can configure any VLAN as an RSPAN VLAN as long as these conditions are met:
 - The same RSPAN VLAN is used for an RSPAN session in all the switches.
 - All participating switches have appropriate hardware and software.
 - No access port (including the sc0 interface) is configured in the RSPAN VLAN.
- If VLAN Trunk Protocol (VTP) and VTP pruning are enabled, RSPAN traffic is pruned in the trunks to prevent the unwanted flooding of RSPAN traffic across the network.
- If GARP VLAN Registration Protocol (GVRP) is enabled and GVRP requests conflict with existing RSPAN VLANs, unwanted traffic might be observed in the respective RSPAN sessions.
- RSPAN VLANs can be used in Inter-Switch Link (ISL) to dot1q mapping. However, ensure that the special properties of RSPAN VLANs are supported in all the switches involved to avoid unwanted traffic in these VLANs.

Configuring RSPAN from the CLI

The first step in configuring an RSPAN session is to select an RSPAN VLAN for the RSPAN session that *does not* exist 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.

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.

Once the RSPAN VLAN is created, you configure the source and destination switches using the **set rspan** command.

To configure RSPAN VLANs, perform this task in privileged mode:

	Task	Command
Step 1	Configure RSPAN VLANs.	set vlan <i>vlan_num</i> [rspan]
Step 2	Verify the RSPAN VLAN configuration.	show vlan

This example shows how to set VLAN 500 as an RSPAN VLAN:

```

Console> (enable) set vlan 500 rspan
vlan 500 configuration successful
Console> (enable)
Console> (enable) show vlan
.
display truncated
.
VLAN DynCreated  RSPAN
-----
1    static      disabled
2    static      disabled
3    static      disabled
99   static      disabled
500  static      enabled
Console> (enable)

```

To configure RSPAN source ports, perform this task in privileged mode:

	Task	Command
Step 1	Configure RSPAN source ports. Use this command on each of the source switches participating in RSPAN.	set rspan source { <i>mod/ports...</i> <i>vlangs...</i> sc0 } { <i>rspan_vlan</i> } [rx tx both] [multicast { enable disable }] [filter <i>vlangs...</i>] [create]
Step 2	Verify the RSPAN configuration.	show rspan

This example shows how to specify ports 4/1 and 4/2 as ingress source ports for RSPAN VLAN 500:

```

Console> (enable) set rspan source 4/1-2 500 rx
Rspan Type      : Source
Destination     : -
Rspan Vlan      : 500
Admin Source    : Port 4/1-2
Oper Source     : None
Direction      : receive
Incoming Packets: -
Learning       : -
Multicast       : enabled
Filter          : -
Console> (enable)

```

To configure RSPAN source VLANs, perform this task in privileged mode:

	Task	Command
Step 1	Configure RSPAN source VLANs. All the ports in the source VLAN become operational source ports.	set rspan source { <i>mod/ports...</i> <i>vlangs...</i> sc0 } { <i>rspan_vlan</i> } [rx tx both] [multicast { enable disable }] [filter <i>vlangs...</i>] [create]
Step 2	Verify the RSPAN configuration.	show rspan

This example shows how to specify VLAN 200 as a source VLAN for RSPAN VLAN 500 (selecting the **rx** option makes all ports in the VLAN ingress ports):

```
Console> (enable) set rspan source 200 500 rx
Rspan Type      : Source
Destination     : -
Rspan Vlan      : 500
Admin Source    : VLAN 200
Oper Source     : None
Direction      : receive
Incoming Packets: -
Learning        : -
Multicast       : enabled
Filter          : -
Console> (enable)
```

To configure RSPAN destination ports, perform this task in privileged mode:

	Task	Command
Step 1	Configure RSPAN destination ports. Use this command on each of the destination switches participating in RSPAN.	set rspan destination { <i>mod_num/port_num</i> } { <i>rspan_vlan</i> } [inpkts { enable disable }] [learning { enable disable }] [create]
Step 2	Verify the RSPAN configuration.	show rspan

```
Console> (enable) set rspan destination 3/1 500
Rspan Type      : Destination
Destination     : Port 3/1
Rspan Vlan      : 500
Admin Source    : -
Oper Source     : -
Direction      : -
Incoming Packets: disabled
Learning        : enabled
Multicast       : -
Filter          : -
Console> (enable)
```

To disable RSPAN, perform this task in privileged mode:

Task	Command
Disable RSPAN on the switch.	set rspan disable source [<i>rspan_vlan</i> all] set rspan disable destination [<i>mod_num/port_num</i> all]

This example shows how to disable all enabled source sessions:

```
Console> (enable) set rspan disable source all
This command will disable all remote span source session(s).
Do you want to continue (y/n) [n]? y
Disabled monitoring of all source(s) on the switch for remote span.
Console> (enable)
```

This example shows how to disable one source session by *rspan_vlan* number:

```
Console> (enable) set rspan disable source 903
Disabled monitoring of all source(s) on the switch for rspan_vlan 903.
Console> (enable)
```

This example shows how to disable all enabled destination sessions:

```
Console> (enable) set rspan disable destination all
This command will disable all remote span destination session(s).
Do you want to continue (y/n) [n]? y
Disabled monitoring of remote span traffic for all rspan destination ports.
Console> (enable)
```

This example shows how to disable one destination session by *mod_num/port_num*:

```
Console> (enable) set rspan disable destination 4/1
Disabled monitoring of remote span traffic on port 4/1.
Console> (enable)
```

RSPAN Configuration Examples

The following sections describe typical RSPAN configurations.

Configuring a Single RSPAN Session

This example shows how to configure a single RSPAN session. Figure 32-3 shows an RSPAN configuration; see Table 32-2 for the necessary commands to configure this RSPAN session. Table 32-2 assumes that you have already set up RSPAN VLAN 901 for this session on all the switches using the **set vlan *vlan_num* rspan** command. 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. Note that in the configuration example shown in Table 32-2, the RSPAN session may be disabled in Switch A or B and both without modifying the configuration in Switch C or Switch D.

Figure 32-3 Single RSPAN Session

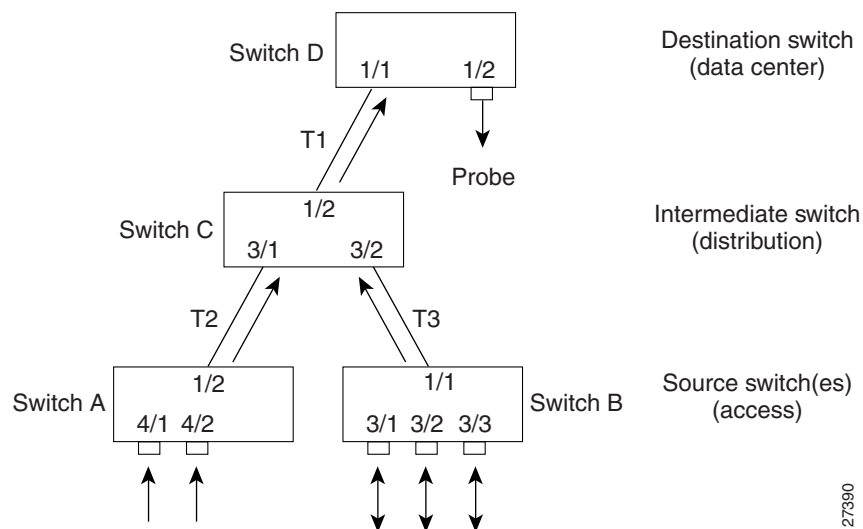


Table 32-2 Configuring a Single RSPAN Session

Switch	Ports	RSPAN VLAN	Direction	RSPAN CLI Commands
A (source)	4/1, 4/2	901	Ingress	set rspan source 4/1-2 901 rx
B (source)	3/1, 3/2, 3/3	901	Bidirectional	set rspan source 3/1-3 901
C (intermediate)	–	901	–	No RSPAN CLI command needed
D (destination)	1/2	901	–	set rspan destination 1/2 901

Modifying an Active RSPAN Session

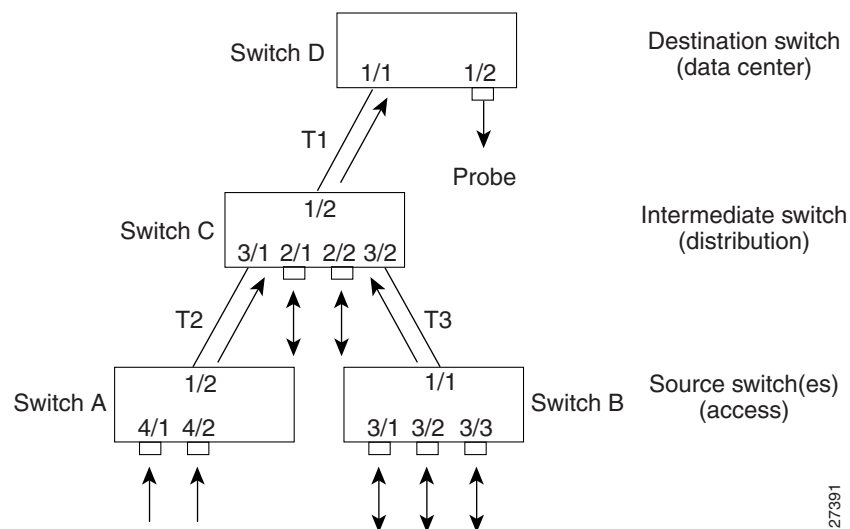
This example shows how to modify an active RSPAN session. Use Figure 32-3 for reference; see Table 32-3 for the necessary commands to disable an RSPAN session and to add or remove source ports from an RSPAN session.

Table 32-3 Making Modifications to an Active RSPAN Session

Switch	Action	RSPAN CLI Commands
A (source)	Disable the RSPAN session.	set rspan disable source 901
B (source)	Remove source port 3/2 from RSPAN session.	set rspan source 3/1, 3/3 901
B (source)	Add back source port 3/2 to RSPAN session.	set rspan source 3/1-3 901

Adding RSPAN Source Ports in Intermediate Switches

This example shows how to add RSPAN source ports in intermediate switches. Figure 32-4 shows an RSPAN configuration; see Table 32-4 for the necessary commands to configure this RSPAN session. Ports 2/1-2 in Switch C can be configured for the same RSPAN session.

Figure 32-4 Adding RSPAN Source Ports in Intermediate Switch

27991

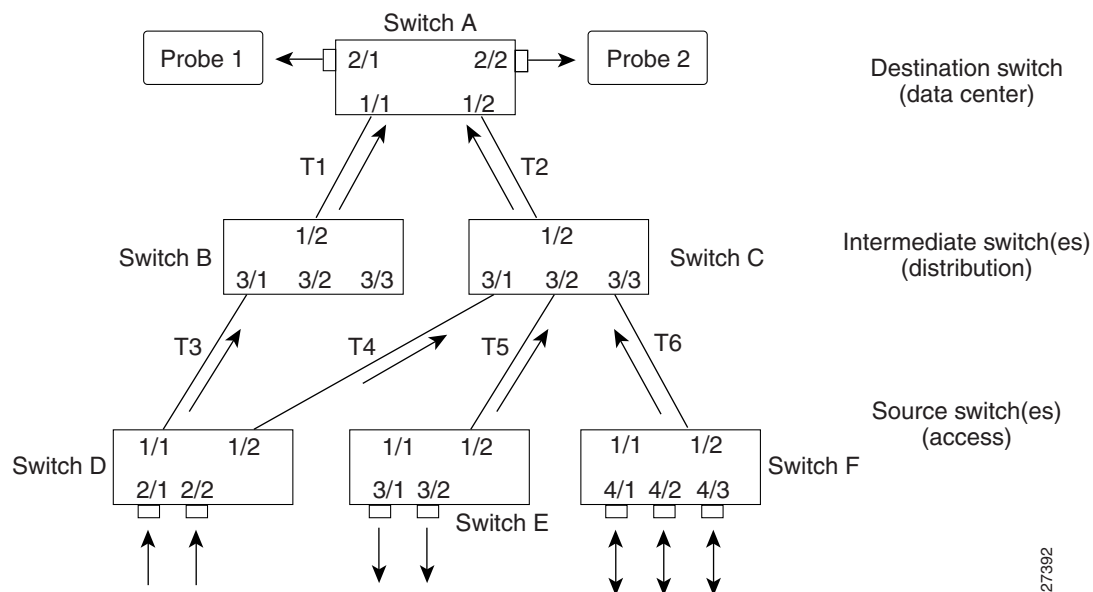
Table 32-4 Adding RSPAN Source Ports in Intermediate Switch

Switch	Ports	RSPAN VLAN	Direction	RSPAN CLI Commands
A (source)	4/1, 4/2	901	Ingress	set rspan source 4/1-2 901 rx
B (source)	3/1, 3/2, 3/3	901	Bidirectional	set rspan source 3/1-3 901
C (intermediate)	–	901	–	No RSPAN CLI command needed
C (source)	2/1, 2/2	901	Bidirectional	set rspan source 2/1-2 901
D (destination)	1/2	901	–	set rspan destination 1/2 901

Configuring Multiple RSPAN Sessions

This example shows how to configure multiple RSPAN sessions. Figure 32-5 shows an RSPAN configuration; see Table 32-5 for the necessary configuration commands to configure this RSPAN session. This is a typical scenario where the monitoring probes would be placed in the data center and source ports in the access switches (other ports in any of the switches can also be configured for RSPAN). If there is no change in the route for SPAN traffic, the destination switch and the intermediate switches need to be configured only once.

In Figure 32-5, two RSPAN sessions are used with RSPAN VLANs 901 (for probe 1) and 902 (for probe 2). The direction of traffic over trunks T1 through T6 is shown only for understanding; the direction of the trunks depends on the STP states of the respective trunks for the RSPAN VLAN(s). You need to configure the RSPAN VLANs in each of the switches for the respective RSPAN sessions. With VTP enabled in the network, you can create the RSPAN VLAN in one switch and VTP propagates it to the other switches in that VTP domain. With VTP disabled, create the RSPAN VLANs in each switch.

Figure 32-5 Configuring Multiple RSPAN Sessions

27392

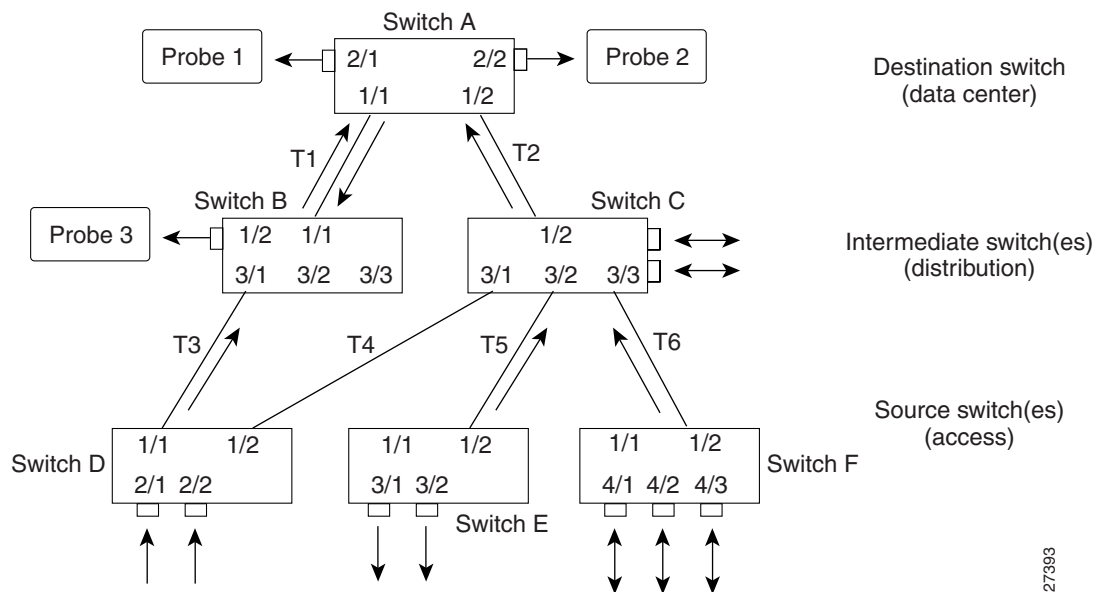
Table 32-5 Configuring Multiple RSPAN Sessions

Switch	Port	RSPAN VLAN(s)	Direction	RSPAN CLI Commands
A (destination)	2/1	901	–	set rspan destination 2/1 901
A (destination)	2/2	902	–	set rspan destination 2/2 902
B (intermediate)	–	901, 902	–	No RSPAN CLI command needed
C (intermediate)	–	901, 902	–	No RSPAN CLI command needed
D (source)	2/1-2	901	Ingress	set rspan source 2/1-2 901 rx
E (source)	3/1-2	901	Egress	set rspan source 3/1-2 901 tx
F (source)	4/1-3	901	Both	set rspan source 4/1-3 902

Adding Multiple Network Analyzers to an RSPAN Session

You can attach multiple network analyzers (probes) to the same RSPAN session. For example, in Figure 32-6, you can add probe 3 in Switch B to monitor RSPAN VLAN 901 using the **set rspan destination 1/2 901** command. Similarly, you could add source ports to Switch C.

Figure 32-6 Adding Multiple Probes to an RSPAN Session



27393