



Configuring SPAN and RSPAN

This chapter describes how to configure the Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) on the Catalyst 4000 family switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference—Catalyst 4000 Family, Catalyst 2948G, and Catalyst 2980G Switches*.

This chapter consists of these major sections:

- [Understanding How SPAN and RSPAN Work, page 26-1](#)
- [SPAN and RSPAN Session Limits, page 26-4](#)
- [Configuring SPAN, page 26-4](#)
- [Configuring RSPAN, page 26-8](#)



Note

To configure SPAN or RSPAN from a Network Management System (NMS), refer to the NMS documentation (and see the [“Using CiscoWorks2000” section on page 24-16](#)).

Understanding How SPAN and RSPAN Work

These sections describe the concepts and terminology associated with SPAN and RSPAN configuration:

- [SPAN Session, page 26-2](#)
- [Destination Port, page 26-2](#)
- [Source Port, page 26-2](#)
- [Reflector Port, page 26-3](#)
- [Ingress SPAN, page 26-3](#)
- [Egress SPAN, page 26-3](#)
- [VSPAN, page 26-3](#)
- [Trunk VLAN Filtering, page 26-4](#)
- [SPAN Traffic, page 26-4](#)

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 that 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.

After the system is on, a SPAN or RSPAN destination session remains inactive 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. After 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” section on page 26-6 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 or a reflector 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 have the encapsulation specified by the trunk type; however, the destination port stops trunking. The **show trunk** command reflects 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 and reflector port, if they belong to any of the administrative source VLANs, are 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 or reflector port for any SPAN session.

If a SPAN session is inactive, the “oper source” field does not update until the session becomes active.

You can configure trunk ports as source ports and mix them with nontrunk source ports; however, the trunk settings of the destination port during SPAN session configuration determine the encapsulation of the packets forwarded by the destination port.

Reflector Port

The reflector port is the mechanism you use to copy 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.

If the bandwidth of the reflector port is not sufficient to handle the traffic 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. A blocking gigabit port reflects at a slightly lower rate.

The reflector port cannot be an EtherChannel port, does not trunk, and cannot do protocol filtering. 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. Spanning tree is automatically disabled on a reflector port; the port remains in the forwarding state even though the port is in loopback mode.

The following ports cannot be used as reflector ports:

- Gigabit uplink ports on the WS-4013 Supervisor II
- Gigabit uplink ports on the 2980G-A
- Gigabit ports on the WS-4232-L3 module

The **SPAN** line in the output of the **show port capabilities** command indicates whether a port can be used as a reflector port.

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

You can use VLAN-based SPAN (VSPAN) to analyze the network traffic in one or more VLANs. You can configure VSPAN in a bi-directional mode (ingress and egress). All the ports in the source VLANs become operational source ports for the VSPAN session. The destination port or the reflector port, if they belong to any of the administrative source VLANs, are excluded from the operational source. If you add or remove ports from the administrative source VLANs, the operational sources modify 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.
- 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

In software release 6.3(1) and later releases, you can use the **filter** option to select a set of VLANs in a trunk used in a SPAN session. Trunk VLAN filtering is the analysis of network traffic on a selected set of VLANs on trunk source ports. If you specify a set of VLANs with the **filter** option, the traffic spanned by the session is limited to the VLANs specified. 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.

Trunk VLAN filtering is available for local SPAN sessions and RSPAN sessions.

SPAN Traffic

All network traffic, including multicast and bridge protocol data unit (BPDU) packets, can be monitored using SPAN (RSPAN does not support monitoring of BPDU packets).

SPAN and RSPAN Session Limits

You can configure (and store in NVRAM) up to five SPAN sessions in a Catalyst 4000 family switch: the five sessions can be split any way between SPAN, RSPAN source, and RSPAN destination sessions.

Configuring SPAN

These sections describe how to configure SPAN:

- [Understanding How SPAN Works, page 26-5](#)
- [SPAN Configuration Guidelines, page 26-5](#)
- [Configuring SPAN, page 26-6](#)

- Any traffic between two network nodes attached to a switch port configured as a SPAN source port is not mirrored to the SPAN destination port. You can span local traffic that passes through the switch.
- You can have up to five SPAN sessions running at the same time with any combination of ingress and egress sessions.

Configuring SPAN

To configure SPAN, perform this task in privileged mode:

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



Caution

If the SPAN destination port is connected to another device and reception of incoming packets is enabled (using the **inpkts enable** keywords), the SPAN destination port receives traffic for the VLAN that the SPAN destination port belongs to. However, the SPAN destination port does *not* participate in spanning tree for that VLAN, so avoid creating network loops with the SPAN destination port.

This example shows how to configure SPAN so that both the transmit and receive traffic from port 2/4 (the SPAN source) is mirrored on port 3/6 (the SPAN destination):

```

Console> (enable) set span 2/4 3/6
Overwrote Port 3/6 to monitor transmit/receive traffic of Port 2/4
Incoming Packets disabled. Learning enabled.
Console> (enable) show span

Destination      : Port 3/6
Admin Source     : Port 2/4
Oper Source      : None
Direction        : transmit/receive
Incoming Packets: disabled
Learning         : enabled
Filter           : -
Status           : active

-----
Total local span sessions: 1
Console> (enable)

```

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
Overwrote Port 2/1 to monitor transmit/receive traffic of VLAN 522
Incoming Packets disabled. Learning enabled.
Console> (enable) show span

Destination      : Port 2/1
Admin Source     : VLAN 522
Oper Source      : Port 2/1-2
Direction        : transmit/receive

```

```
Incoming Packets: disabled
Learning       : enabled
Filter        : -
Status       : active
```

```
-----
Total local span sessions: 1
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
Overwrote Port 2/12 to monitor transmit/receive traffic of VLAN 522
Incoming Packets enabled. Learning enabled.
Console> (enable) show span
Destination      : Port 2/12
Admin Source     : VLAN 522
Oper Source      : Port 2/1-2
Direction        : transmit
Incoming Packets: enabled
Filter           : -
Status           : active
```

```
-----
Total local span sessions: 1
Console> (enable)
```

This example shows how to set multiple SPAN sessions using the following configurations:

- Port 3/1 as the SPAN source and port 2/3 as the SPAN destination
- Port 3/2 as the SPAN source and port 2/5 as the SPAN destination

```
Console> (enable) set span 3/1 2/3
Overwrote Port 2/3 to monitor transmit/receive traffic of Port 3/1
Incoming Packets disabled. Learning enabled.
Console> (enable) set span 3/2 2/5 tx create
Created Port 2/5 to monitor transmit traffic of Port 3/2
Incoming Packets disabled. Learning enabled.
Console> (enable) show span

Destination      : Port 2/3
Admin Source     : Port 3/1
Oper Source      : None
Direction        : transmit/receive
Incoming Packets: disabled
Learning         : enabled
Filter           : -
Status           : inactive
```

```
-----
Destination      : Port 2/5
Admin Source     : Port 3/2
Oper Source      : None
Direction        : transmit
Incoming Packets: disabled
Learning         : enabled
Filter           : -
Status           : inactive
```

```
-----
Total local span sessions: 2
Console> (enable)
```

This example shows how to configure SPAN so that both transmit and receive traffic from the trunking port 3/4 (the SPAN source) are mirrored on port 3/5 (the SPAN destination) and both VLANs 50 and 850 are filtered:

```

Console> (enable) set span 3/4 3/5 both filter 50,850
Overwrote Port 3/5 to monitor transmit/receive traffic of Port 3/4
Incoming Packets disabled. Learning enabled.
Console> (enable) show span

Destination      : Port 3/5
Admin Source     : Port 3/4
Oper Source      : None
Direction        : transmit/receive
Incoming Packets : disabled
Learning         : enabled
Filter           : 50,850
Status           : inactive

-----
Total local span sessions: 1
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 2/3
This command may disable your span session(s).
Do you want to continue (y/n) [n]? y
Disabled Port 2/3 to monitor transmit/receive traffic of Port
Incoming Packets disabled. Learning enabled.
Console> (enable)

```

Configuring RSPAN

These sections describe how to configure RSPAN:

- [RSPAN Software and Hardware Requirements, page 26-8](#)
- [Understanding How RSPAN Works, page 26-9](#)
- [RSPAN Configuration Guidelines, page 26-10](#)
- [Configuring RSPAN, page 26-11](#)
- [RSPAN Configuration Examples, page 26-14](#)

RSPAN Software and Hardware Requirements

You must have software release 6.3(1) or a later release to use the RSPAN functionality on the Catalyst 4000 family switches or to use a Catalyst 4000 family switch as an intermediate switch in an RSPAN session.

RSPAN supervisor engine requirements are as follows:

- For source switches—Any Catalyst 4000 family switch supervisor engine
- For destination or intermediate switches—Any Catalyst 4000 family or Catalyst 6500 series switch supervisor engine

You cannot place any third-party or other Cisco switches in the end-to-end path for RSPAN traffic.

Understanding How RSPAN Works



Note

See the “[Understanding How SPAN and RSPAN Work](#)” section on page 26-1 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 26-5), plus support for source ports and destination ports distributed across multiple switches, allowing remote monitoring of multiple switches across your network.

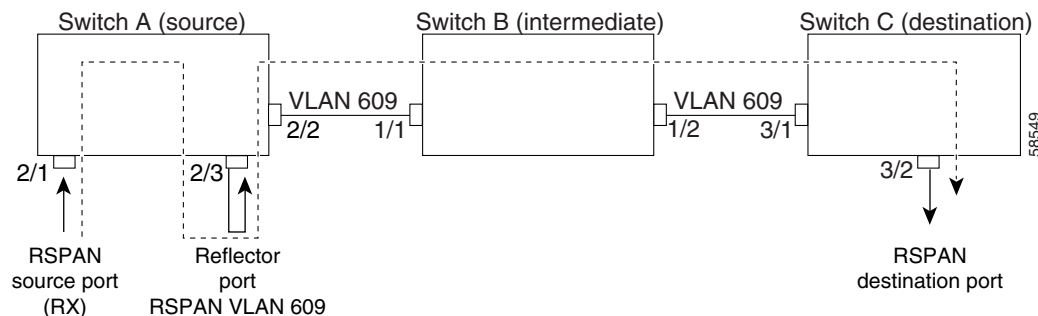
The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The SPAN traffic from the sources is copied onto the RSPAN VLAN through the reflector port and then forwarded over trunk ports carrying the RSPAN VLAN to RSPAN destination ports monitoring the RSPAN VLAN.

Traffic sent out through the source port is also sent out on the reflector port. Because the reflector port is an access (non-trunking) port in loopback mode, the traffic is switched out with no VLAN tag and is immediately sent back to the switch. In the loopback, the traffic is encoded into the RSPAN VLAN. A switch with an RSPAN destination session receives the traffic (see [Figure 26-2](#)).

The traffic type for sources (ingress, egress, or both) in an RSPAN session can be different for source switches, but must be the same for all source ports on a given switch.

Do not configure any ports in an RSPAN VLAN except those selected to carry RSPAN traffic. Learning is disabled on the RSPAN VLAN.

Figure 26-2 Flow of RSPAN Monitored Traffic



RSPAN Configuration Guidelines

This section lists the guidelines for configuring RSPAN:



Tip

Because 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.

- All the items in the “[SPAN Configuration Guidelines](#)” section on page 26-5 apply to RSPAN.
- RSPAN sessions can coexist with SPAN sessions to a maximum of five sessions. The limit on the number of sessions the Catalyst 4000 family switches can carry as an intermediate switch is the maximum number of VLANs for the switch.
- For RSPAN configuration, you can distribute the source ports and the destination port across multiple switches.
- A port cannot serve as an RSPAN source port or RSPAN destination port while designated as an RSPAN reflector port.
- 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 the same VLAN. With RSPAN, the traffic is forwarded to remote switches in the RSPAN VLAN. The RSPAN VLAN is configured only on trunk ports, not on access ports.
- The learning option applies to RSPAN destination ports only.
- RSPAN does not support BPDU packet monitoring.
- RSPAN VLANs are not 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 you enable VLAN Trunk Protocol (VTP) and VTP pruning, RSPAN traffic is pruned in the trunks to prevent the unwanted flooding of RSPAN traffic across the network.
- If you enable GARP VLAN Registration Protocol (GVRP) and GVRP requests conflict with existing RSPAN VLANs, you might observe unwanted traffic in the respective RSPAN sessions.
- You can use RSPAN VLANs in Inter-Switch Link (ISL) to map dot1q. However, ensure that the special properties of RSPAN VLANs are supported in all the switches to avoid unwanted traffic in these VLANs.
- Incoming traffic on the RSPAN destination port is disabled by default. You can enable it using the **inpkts enable** keywords. However, while the port receives traffic for its assigned VLAN, it does not participate in spanning tree for that VLAN. To avoid creating spanning tree loops with incoming traffic enabled, assign the RSPAN destination port to an unused VLAN.
- When the **inpkts** option is enabled, you can prevent the switch from learning source MAC addresses from traffic received on the RSPAN destination port using the **learning disable** keywords. If you want the switch to learn source MAC addresses from traffic received on the RSPAN destination port, use the **learning enable** keywords. By default, the switch learns source MAC addresses from incoming traffic (**learning enable**) if the **inpkts** option is enabled. The source MAC address learning options only affect traffic received from a device attached to the RSPAN destination port itself, not from traffic mirrored from the RSPAN source.

Configuring RSPAN

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> } { <i>rspan_vlan</i> } reflector <i>mod/port</i> [rx tx both] [filter <i>vlangs...</i>] [create]
Step 2	Verify the RSPAN configuration.	show rspan

This example shows how to specify port 2/3 as an ingress source port for RSPAN VLAN 500 with port 2/34 as the reflector port:

```

Console> (enable) set rspan source 2/3 500 reflector 2/34 rx
Rspan Type      : Source
Destination     : -
Reflector       : Port 2/34
Rspan Vlan      : 500
Admin Source    : Port 2/3
Oper Source     : Port 2/3
Direction      : receive

```

```
Incoming Packets: -
Learning         : -
Filter           : -
Status           : active
```

```
Console> (enable) 2001 May 02 13:22:17 %SYS-5-SPAN_CFGSTATECHG:remote span source session
active for remote span vlan 500
```

This example shows how to specify port 2/3 as a source port for RSPAN VLAN 500 with port 2/34 as the reflector port and to filter VLANs 50 and 850:

```
Console> (enable) set rspan source 2/3 500 reflector 2/34 filter 50,850
Rspan Type       : Source
Destination      : -
Reflector        : Port 2/34
Rspan Vlan       : 500
Admin Source     : Port 2/3
Oper Source      : Port 2/3
Direction        : transmit/receive
Incoming Packets: -
Learning         : -
Filter           : 50,850
Status           : active
```

```
Console> (enable) 2001 May 02 13:25:59 %SYS-5-SPAN_CFGSTATECHG:remote span source session
active for remote span vlan 500
```

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> } { <i>rspan_vlan</i> } reflector <i>mod/port</i> [rx tx both] [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:

```
Console> (enable) set rspan source 200 500
Rspan Type       : Source
Destination      : -
Rspan Vlan       : 500
Admin Source     : VLAN 200
Oper Source      : None
Direction        : transmit/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

**Caution**

If the RSPAN destination port is connected to another device and reception of incoming packets is enabled (using the **inpkts enable** keywords), the RSPAN destination port receives traffic for the VLAN to which the RSPAN destination port belongs. However, the RSPAN destination port does *not* participate in spanning tree for that VLAN, so avoid creating network loops with the RSPAN destination port.

This example shows how to specify port 3/1 as the RSPAN destination port in VLAN 500:

```
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
Filter          : -
Status          : active
Console> (enable)
```

Disabling RSPAN Sessions

When disabling an RSPAN session, you must disable all source and destination sessions on all participating switches. Leaving RSPAN source sessions enabled consumes bandwidth with RSPAN VLAN traffic.

To disable RSPAN, perform this task in privileged mode:

	Task	Command
Step 1	Disable RSPAN source sessions on the switch.	set rspan disable source [<i>rspan_vlan</i> all]
Step 2	Disable RSPAN destination sessions on the switch.	set rspan disable destination [<i>mod_num/port_num</i> all]

This example shows how to disable all enabled source sessions on the switch:

```
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 on the switch:

```
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

These sections provide examples that show how to configure RSPAN:

- [Configuring a Single RSPAN Session, page 26-14](#)
- [Modifying an Active RSPAN Session, page 26-15](#)
- [Adding RSPAN Source Ports in Intermediate Switches, page 26-15](#)
- [Configuring Multiple RSPAN Sessions, page 26-16](#)
- [Adding Multiple Network Analyzers to an RSPAN Session, page 26-17](#)
- [Disabling the RSPAN Session, page 26-17](#)

Configuring a Single RSPAN Session

This example shows how to configure a single RSPAN session. [Figure 26-3](#) shows an RSPAN configuration; see [Table 26-1](#) for the necessary commands to configure this RSPAN session. [Table 26-1](#) 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 26-1](#), the RSPAN session may be disabled in Switch A or B or both without modifying the configuration in Switch C or Switch D.

Figure 26-3 Single RSPAN Session

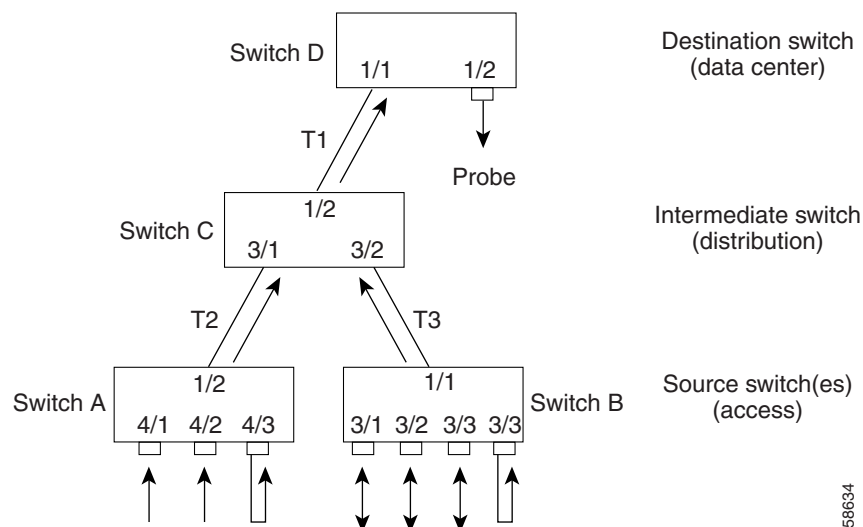


Table 26-1 Configuring a Single RSPAN Session

Switch	Ports	Reflector Port	RSPAN VLAN	Direction	RSPAN CLI Commands
A (source)	4/1, 4/2	4/3	901	Ingress	set rspan source 4/1-2 901 rx reflector 4/3
B (source)	3/1, 3/2, 3/3	3/4	901	Bidirectional	set rspan source 3/1-3 901 reflector 3/4
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 26-3](#) for reference; see [Table 26-2](#) for the necessary commands to disable an RSPAN session and to add or remove source ports from an RSPAN session.

Table 26-2 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 reflector 3/4
B (source)	Add source port 3/2 to RSPAN session.	set rspan source 3/1-3 901 reflector 3/4

Adding RSPAN Source Ports in Intermediate Switches

This example shows how to add RSPAN source ports in intermediate switches. [Figure 26-4](#) shows an RSPAN configuration; see [Table 26-3](#) for the necessary commands to configure this RSPAN session. Ports 2/1-2 in Switch C can be configured for the same RSPAN session.

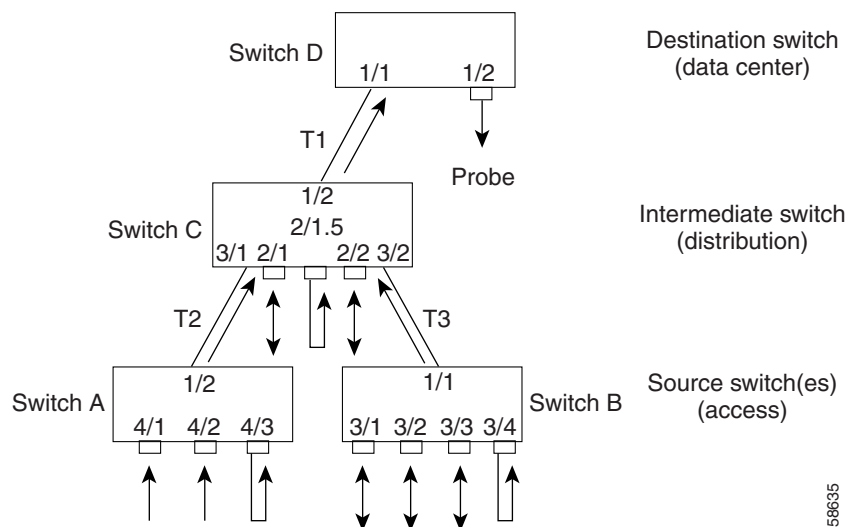
Figure 26-4 Adding RSPAN Source Ports in Intermediate Switch

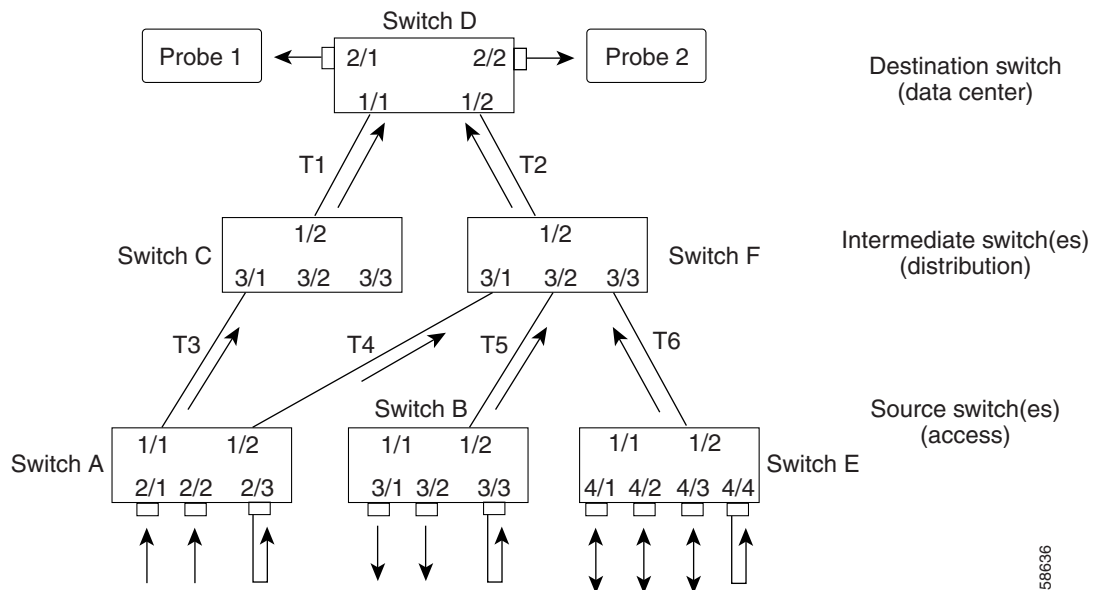
Table 26-3 Adding RSPAN Source Ports in Intermediate Switch

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

Configuring Multiple RSPAN Sessions

This example shows how to configure multiple RSPAN sessions. [Figure 26-5](#) shows an RSPAN configuration; see [Table 26-4](#) 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 26-5](#), 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 26-5 Configuring Multiple RSPAN Sessions

58636

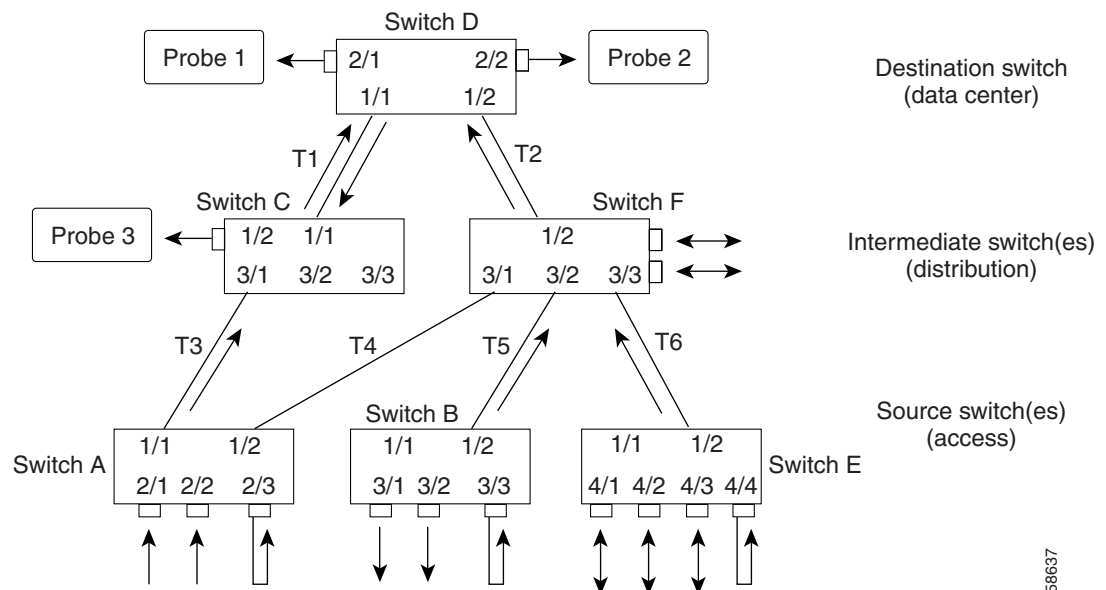
Table 26-4 Configuring Multiple RSPAN Sessions

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

Adding Multiple Network Analyzers to an RSPAN Session

You can attach multiple network analyzers (probes) to the same RSPAN session. For example, in [Figure 26-6](#), 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 26-6 Adding Multiple Probes to an RSPAN Session



Disabling the RSPAN Session

To completely disable the previous RSPAN session, you need to disable every RSPAN source and RSPAN destination on each source and destination switch. [Table 26-5](#) lists the commands necessary to completely disable the RSPAN session.

Table 26-5 *Disabling the RSPAN Sessions*

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