CHAPTER 52

Monitoring Network Traffic Using SPAN

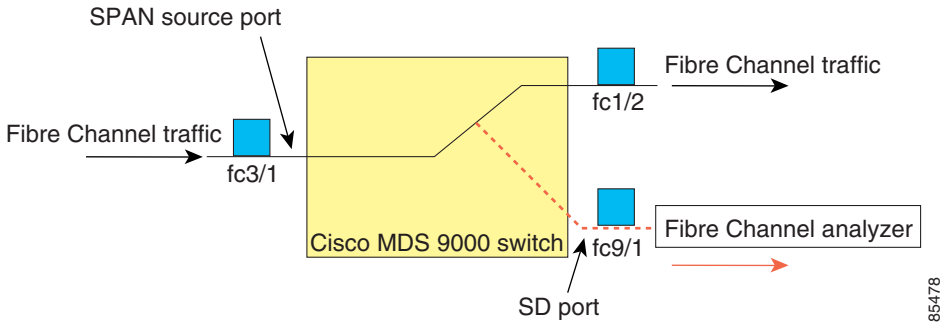
This chapter describes the Switched Port Analyzer (SPAN) features provided in switches in the Cisco MDS 9000 Family. It includes the following sections:

About SPAN

The SPAN feature is specific to switches in the Cisco MDS 9000 Family. It monitors network traffic through a Fibre Channel interface. Traffic through any Fibre Channel interface can be replicated to a special port called the SPAN destination port (SD port). Any Fibre Channel port in a switch can be configured as an SD port. Once an interface is in SD port mode, it cannot be used for normal data traffic. You can attach a Fibre Channel Analyzer to the SD port to monitor SPAN traffic (see the"Cisco Fabric Analyzer" section on page 58-4.

SD ports do not receive frames, they merely transmit a copy of the SPAN source traffic. The SPAN feature is non-intrusive and does not affect switching of network traffic for any SPAN source ports (see Figure 52-1).

Figure 52-1 SPAN Transmission

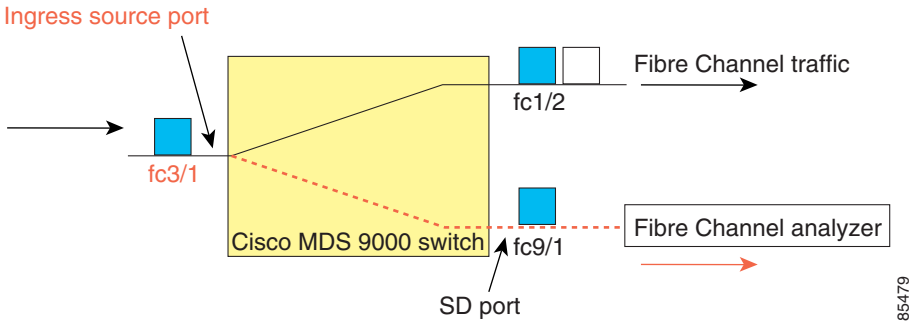


SPAN Sources

SPAN sources refer to the interfaces from which traffic can be monitored. You can also specify VSAN as a SPAN source, in which case, all supported interfaces in the specified VSAN are included as SPAN sources. You can choose the SPAN traffic in the ingress direction, the egress direction, or both directions for any source interface:

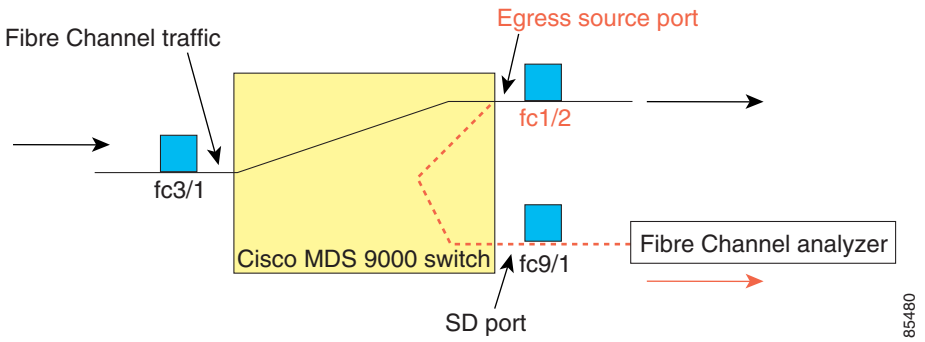
- Ingress source (Rx)—Traffic entering the switch fabric through this source interface is *spanned* or copied to the SD port (see Figure 52-2).

Figure 52-2 SPAN Traffic from the Ingress Direction



- Egress source (Tx)—Traffic exiting the switch fabric through this source interface is spanned or copied to the SD port (see Figure 52-3).

Figure 52-3 SPAN Traffic from Egress Direction



IPS Source Ports

SPAN capabilities are available on the IP Storage Services (IPS) module. The SPAN feature is only implemented on the FCIP and iSCSI virtual Fibre Channel port interfaces, not the physical Gigabit Ethernet ports. You can configure SPAN for ingress traffic, egress traffic, or traffic in both directions for all eight iSCSI and 24 FCIP interfaces that are available in the IPS module.

Note You can configure SPAN for Ethernet traffic using Cisco switches or routers connected to the Cisco MDS 9000 Family IPS modules.

Allowed Source Interface Types

The SPAN feature is available for the following interface types:

- Physical ports such as F ports, FL ports, TE ports, E ports, and TL ports.
- Interface sup-fc0 (traffic to and from the supervisor):
  - The Fibre Channel traffic from the supervisor module to the switch fabric through the sup-fc0 interface is called ingress traffic. It is spanned when sup-fc0 is chosen as an ingress source port.
  - The Fibre Channel traffic from the switch fabric to the supervisor module through the sup-fc0 interface is called egress traffic. It is spanned when sup-fc0 is chosen as an egress source port.
- PortChannels
  - All ports in the PortChannel are included and spanned as sources.
  - You cannot specify individual ports in a PortChannel as SPAN sources. Previously configured SPAN-specific interface information is discarded.
- IPS module specific Fibre Channel interfaces:
  - iSCSI interfaces
  - FCIP interfaces

VSAN as a Source

When a VSAN as a source is specified, then all physical ports and PortChannels in that VSAN are included as SPAN sources. A TE port is included only when the port VSAN of the TE port matches the source VSAN. A TE port is excluded even if the configured allowed VSAN list may have the source VSAN, but the port VSAN is different.

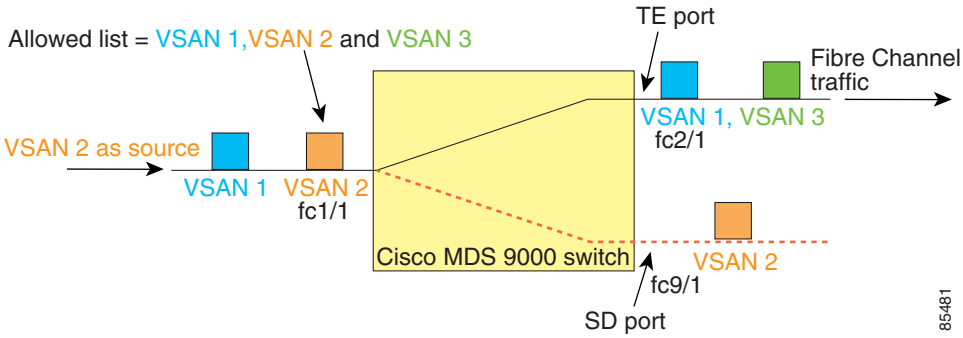
You cannot configure source interfaces (physical interfaces, PortChannels, or sup-fc interfaces) and source VSANs in the same SPAN session.

Guidelines to Configure VSANs as a Source

The following guidelines apply when configuring VSANs as a source:

- Traffic on all interfaces included in a source VSAN is spanned only in the ingress direction.
- If a VSAN is specified as a source, you cannot perform interface-level SPAN configuration on the interfaces that are included in the VSAN. Previously configured SPAN-specific interface information is discarded.
- If an interface in a VSAN is configured as a source, you cannot configure that VSAN as a source. You must first remove the existing SPAN configurations on such interfaces before configuring VSAN as a source.
- Interfaces are only included as sources when the port VSAN matches the source VSAN. Figure 52-4 displays a configuration using VSAN 2 as a source:
  - All ports in the switch are in VSAN 1 except fc1/1.
  - Interface fc1/1 is the TE port with port VSAN 2. VSANs 1, 2, and 3 are configured in the allowed list.
  - VSAN 1 and VSAN 2 are configured as SPAN sources.

Figure 52-4 VSAN as a Source



For this configuration, the following apply:

- VSAN 2 as a source includes only the TE port fc1/1 that has port VSAN 2.
- VSAN 1 as a source does not include the TE port fc1/1 because the port VSAN does not match VSAN 1.

  See the "Configuring an Allowed-Active List of VSANs" section on page 15-6 or the "About Port VSAN Membership" section on page 19-7.

SPAN Sessions

Each SPAN session represents an association of one destination with a set of source(s) along with various other parameters that you specify to monitor the network traffic. One destination can be used by one or more SPAN sessions. You can configure up to 16 SPAN sessions in a switch. Each session can have several source ports and one destination port.

To activate any SPAN session, at least one source and the SD port must be up and functioning. Otherwise, traffic is not directed to the SD port.

Tip A source can be shared by two sessions, however, each session must be in a different direction—one ingress and one egress.

You can temporarily deactivate (suspend) any SPAN session. The traffic monitoring is stopped during this time.

Specifying Filters

You can perform VSAN-based filtering to selectively monitor network traffic on specified VSANs. You can apply this VSAN filter to all sources in a session (see Figure 52-4). Only VSANs present in the filter are spanned.

You can specify session VSAN filters that are applied to all sources in the specified session. These filters are bidirectional and apply to all sources configured in the session.

Guidelines to Specifying Filters

The following guidelines apply to SPAN filters:

- PortChannel configurations are applied to all ports in the PortChannel.
- If no filters are specified, the traffic from all active VSANs for that interface is spanned by default.
- While you can specify arbitrary VSAN filters in a session, traffic can only be monitored on the port VSAN or on allowed-active VSANs in that interface.

SD Port Characteristics

An SD port has the following characteristics:

- Ignores BB_credits.
- Allows data traffic only in the egress (Tx) direction.
- Does not require a device or an analyzer to be physically connected.
- Supports only 1 Gbps or 2 Gbps speeds. The auto speed option is not allowed.
- Multiple sessions can share the same destination ports.
- If the SD port is shut down, all shared sessions stop generating SPAN traffic.
- The outgoing frames can be encapsulated in Extended Inter-Switch Link (EISL) format.

- The SD port does not have a port VSAN.
- SD ports cannot be configured using Storage Services Modules (SSMs).
- The port mode cannot be changed if it is being used for a SPAN session.

Note If you need to change an SD port mode to another port mode, first remove the SD port from all sessions and then change the port mode using the **switchport mode** command.

Guidelines to Configure SPAN

The following guidelines apply for SPAN configurations:

- You can configure up to 16 SPAN sessions with multiple ingress (Rx) sources.
- You can configure a maximum of three SPAN sessions with one egress (Tx) port.
- In a 32-port switching module, you must configure the same session in all four ports in one port group (unit). If you wish, you can also configure only two or three ports in this unit (see the "32-Port Switching Module Configuration Guidelines" section on page 12-2).
- SPAN frames are dropped if the sum of the bandwidth of the sources exceeds the speed of the destination port.
- Frames dropped by a source port are not spanned.

Configuring SPAN

To monitor network traffic using SD ports, follow these steps:

Step 1 Configure the SD port.

Step 2 Attach the SD port to a specific SPAN session.

Step 3 Monitor network traffic by adding source interfaces to the session.

To configure an SD port for SPAN monitoring, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# interface fc9/1`	Configures the specified interface.
Step 3	`switch(config-if)# switchport mode SD`	Configures the SD port mode for interface fc9/1.
Step 4	`switch(config-if)# switchport speed 1000`	Configures the SD port speed to 1000 Mbps.
Step 5	`switch(config-if)# no shutdown`	Enables traffic flow through this interface.

To configure a SPAN session, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# span session 1` `switch(config-span)#`	Configures the specified SPAN session (1). If the session does not exist, it is created.
	`switch(config)# no span session 1`	Deletes the specified SPAN session (1).
Step 3	`switch(config-span)# destination interface fc9/1`	Configures the specified destination interface (fc 9/1) in a session.
	`switch(config-span)# no destination interface fc9/1`	Removes the specified destination interface (fc 9/1).
Step 4	`switch(config-span)# source interface fc7/1`	Configures the source (fc7/1) interface in both directions. **Note** The Cisco MDS 9124 Fabric Switch does not support bi-directional SPAN sessions (Rx and Tx)
	`switch(config-span)# no source interface fc7/1`	Removes the specified destination interface (fc 7/1) from this session.
Step 5	`switch(config-span)# source interface sup-fc0`	Configures the source interface (sup-fc0) in the session.
	`switch(config-span)# source interface fc1/5 - 6, fc2/1 -3`	Configures the specified interface ranges in the session.
	`switch(config-span)# source vsan 1-2`	Configures source VSANs 1 and 2 in the session.
	`switch(config-span)# source interface port-channel 1`	Configures the source PortChannel (port-channel 1).
	`switch(config-span)# source interface fcip 51`	Configures the source FCIP interface in the session.
	`switch(config-span)# source interface iscsi 4/1`	Configures the source iSCSI interface in the session.
	`switch(config-span)# source interface svc1/1 tx traffic-type initiator`	Configures the source SVC interface in the Tx direction for an initiator traffic type.
	`switch(config-span)# no source interface port-channel 1`	Deletes the specified source interface (port-channel 1).

To configure a SPAN filter, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# span session 1` `switch(config-span)#`	Configures the specified session (1).

	Command	Purpose
Step 3	`switch(config-span)# source interface fc9/1 tx`	Configures the source fc9/1 interface in the egress (Tx) direction.
	`switch(config-span)# source filter vsan 1-2`	Configures VSANs 1 and 2 as session filters.
	`switch(config-span)# source interface fc7/1 rx`	Configures the source fc7/1 interface in the ingress (Rx) direction.

Configuring SPAN for Generation 2 Fabric Switches

Cisco Generation 2 Fabric Switches (such as MDS 9124) support single direction (SPAN session 1) SPAN sessions only.

The following example shows how to configure SPAN sessions for the ingress direction for this switch.

Example 52-1 Configuring a Generation 2 Fabric Switch for Ingress SPAN sessions

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# span session 1` `switch(config-span)#`	Configures the specified session (1).
Step 3	`switch(config-span)# destination interface fc1/1`	Configures interface fc1/1 as the destination.
Step 4	`switch(config-span)# source interface fc1/2 rx`	Configures the source interface fc1/2 in the ingress direction.

Example 52-2 Configuring a Generation 2 Fabric Switch for Egress SPAN Session

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# span session 1` `switch(config-span)#`	Configures the specified session (1).
Step 3	`switch(config-span)# destination interface fc1/1`	Configures interface fc1/1 as the destination.
Step 4	`switch(config-span)# source interface fc1/2 tx`	Configures the source interface fc1/2 in the egress direction.

You cannot mix ingress and egress interfaces in the same SPAN session. The SPAN will reject any configuration that mixes Rx ad Tx directions. However, you can specify multiple SPAN source interfaces in a single direction.

Example 52-3 Configuring Cisco MDS 9124 for Multiple SPAN Interfaces in a Single Direction

```
switch(config-span)# span session 1
switch(config-span)# destination interface fc1/1
switch(config-span)# source interface fc1/2 rx
switch(config-span)# source interface fc1/3 rx
```

Generation 2 Fabric Switches support VSAN filters for one VSAN only in the egress direction; this restriction does not apply to the ingress direction. For example, if you have an interface that is a TE port, with an active VSAN of 1 to 5, and you specify a VSAN filter for VSAN 2, then only the traffic on VSAN 2 will be filtered.

```
switch(config-span)# span session 1
switch(config-span)# source filter vsan 2
switch(config-span)# destination interface fc1/1
switch(config-span)# source interface fc1/2 tx
```

However, if you specify the VSAN filter for VSANs 1 to 2, then traffic from all VSANs (1 to 5) is filtered–essentially rendering the filter useless.

```
switch(config-span)# span session 1
switch(config-span)# source filter vsan 1-2
switch(config-span)# destination interface fc1/1
switch(config-span)# source interface fc1/2 tx
```

Suspending and Reactivating SPAN Sessions

You can temporarily deactivate (suspend) any SPAN session. The traffic monitoring is stopped during this time.

To temporarily suspend or reactivate a SPAN session filter, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# span session 1` `switch(config-span)#`	Configures the specified session (1).
Step 3	`switch(config-span)# suspend`	Temporarily suspends the session.
	`switch(config-span)# no suspend`	Reactivates the session.

Note When using Generation 2 Fabric Switches, you cannot create an additional active SPAN session when you already have one.

Encapsulating Frames

The frame encapsulation feature is disabled by default. If you enable the encapsulation feature, all outgoing frames are encapsulated.

The **switchport encap eisl** command only applies to SD port interfaces. If encapsulation is enabled, you see a new line (`Encapsulation is eisl`) in the **show interface** *SD_port_interface* command output.

To encapsulate outgoing frames (optional), follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# interface fc9/32`	Configures the specified interface.

	Command	Purpose
Step 3	`switch(config-if)# switchport mode SD`	Configures the SD port mode for interface fc9/32.
Step 4	`switch(config-if)# switchport encap eisl`	Enables the encapsulation option for this SD port.
	`switch(config-if)# no switchport encap eisl`	Disables (default) the encapsulation option.

SPAN Conversion Behavior

SPAN features (configured in any prior release) are converted as follows:

- If source interfaces and source VSANs are configured in a given session, then all the source VSANs are removed from that session.

  For example, before Cisco MDS SAN-OS Release 1.0(4):

```
Session 1 (active)
   Destination is fc1/9
   No session filters configured
   Ingress (rx) sources are
      vsans 10-11
     fc1/3,
   Egress (tx) sources are
     fc1/3,
```

  Once upgraded to Cisco MDS SAN-OS Release 1.1(1):

```
Session 1 (active)
   Destination is fc1/9
   No session filters configured
   Ingress (rx) sources are
     fc1/3,
   Egress (tx) sources are
     fc1/3,
```

  Session 1 had both source interfaces and source VSANs before the upgrade. After the upgrade, the source VSANs were removed (rule 1).

- If interface level VSAN filters are configured in source interfaces, then the source interfaces are also removed from the session. If this interface is configured in both directions, it is removed from both directions.

  For example, before Cisco MDS SAN-OS Release 1.0(4):

```
Session 2 (active)
   Destination is fc1/9
   No session filters configured
   Ingress (rx) sources are
      vsans 12
     fc1/6 (vsan 1-20),
   Egress (tx) sources are
     fc1/6 (vsan 1-20),
```

  Once upgraded to Cisco MDS SAN-OS Release 1.1(1):

```
Session 2 (inactive as no active sources)
   Destination is fc1/9
   No session filters configured
   No ingress (rx) sources
   No egress (tx) sources
```

Note The deprecated configurations are removed from persistent memory once a switchover or a new startup configuration is implemented.

Session 2 had a source VSAN 12 and a source interface fc1/6 with VSAN filters specified in Cisco MDS SAN-OS Release 1.0(4). When upgraded to Cisco MDS SAN-OS Release 1.1(1) the following changes are made:

- The source VSAN (VSAN 12) is removed (rule 1).
- The source interface fc1/6 had VSAN filters specified—it is also removed (rule 2).

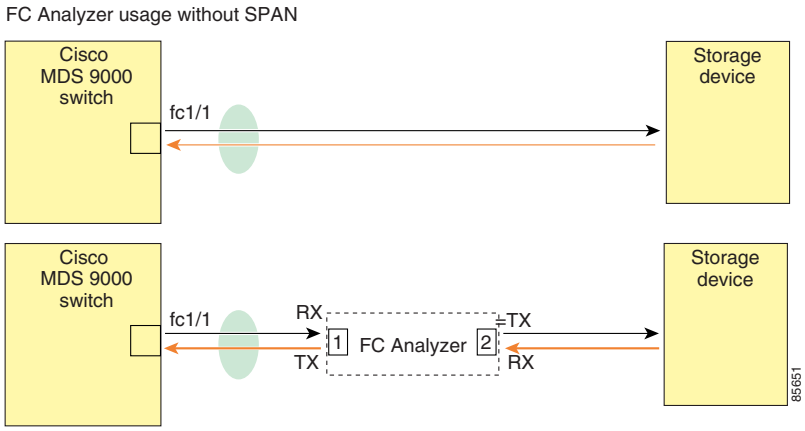
Monitoring Traffic Using Fibre Channel Analyzers

You can use SPAN to monitor traffic on an interface without any traffic disruption. This feature is specially useful in troubleshooting scenarios where traffic disruption changes the problem environment and makes it difficult to reproduce the problem.

Without SPAN

You can monitor traffic using interface fc1/1 in a Cisco MDS 9000 Family switch that is connected to another switch or host. You need to physically connect a Fibre Channel analyzer between the switch and the storage device to analyze the traffic through interface fc1/1 as shown in Figure 52-5.

Figure 52-5 Fibre Channel Analyzer Usage Without SPAN



This type of connection has the following limitations:

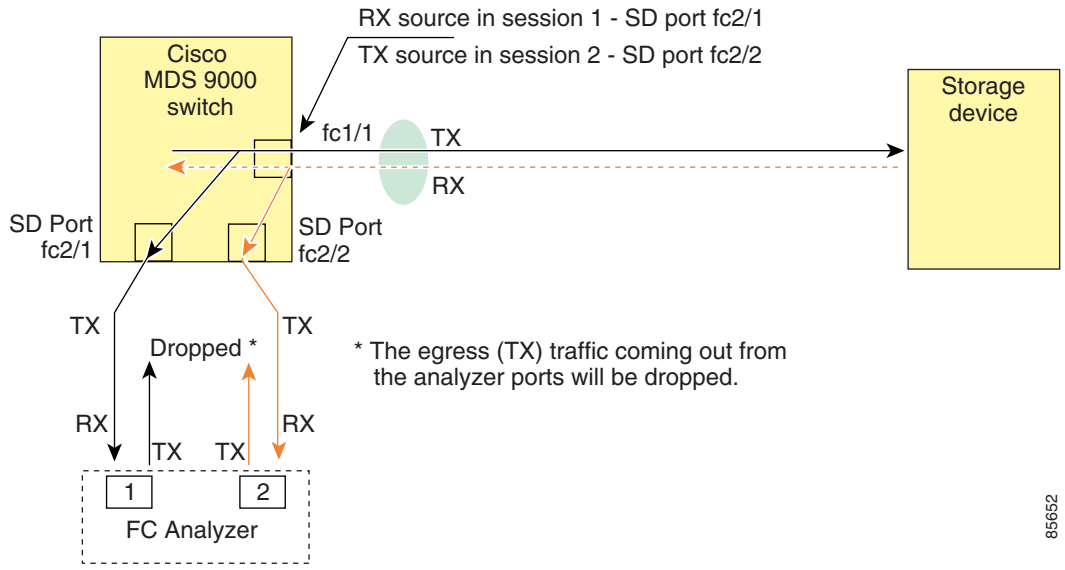
- It requires you to physically insert the FC analyzer between the two network devices.
- It disrupts traffic when the Fibre Channel analyzer is physically connected.
- The analyzer captures data only on the Rx links in both port 1 and port 2. Port 1 captures traffic exiting interface fc1/1 and port 2 captures ingress traffic into interface fc1/1.

With SPAN

Using SPAN you can capture the same traffic scenario shown in Figure 52-5 without any traffic disruption. The Fibre Channel analyzer uses the ingress (Rx) link at port 1 to capture all the frames going out of the interface fc1/1. It uses the ingress link at port 2 to capture all the ingress traffic on interface fc1/1.

Using SPAN you can monitor ingress traffic on fc1/1 at SD port fc2/2 and egress traffic on SD port fc2/1. This traffic is seamlessly captured by the FC analyzer as shown in Figure 52-6.

Figure 52-6 Fibre Channel Analyzer Using SPAN



Configuring Fibre Channel Analyzers Using SPAN

To configure Fibre Channel Analyzers using SPAN for the example in Figure 52-6, follow these steps:

Step 1 Configure SPAN on interface fc1/1 in the ingress (Rx) direction to send traffic on SD port fc2/1 using session 1.

Step 2 Configure SPAN on interface fc1/1in the egress (Tx) direction to send traffic on SD port fc2/2 using session 2.

Step 3 Physically connect fc2/1 to port 1 on the Fibre Channel analyzer.

Step 4 Physically connect fc2/2 to port 2 on the Fibre Channel analyzer.

To configure SPAN on the source and destination interfaces, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# span session 1` `switch(config-span)#`	Creates the SPAN session 1.
Step 3	`switch(config-span)## destination interface fc2/1`	Configures the destination interface fc2/1.

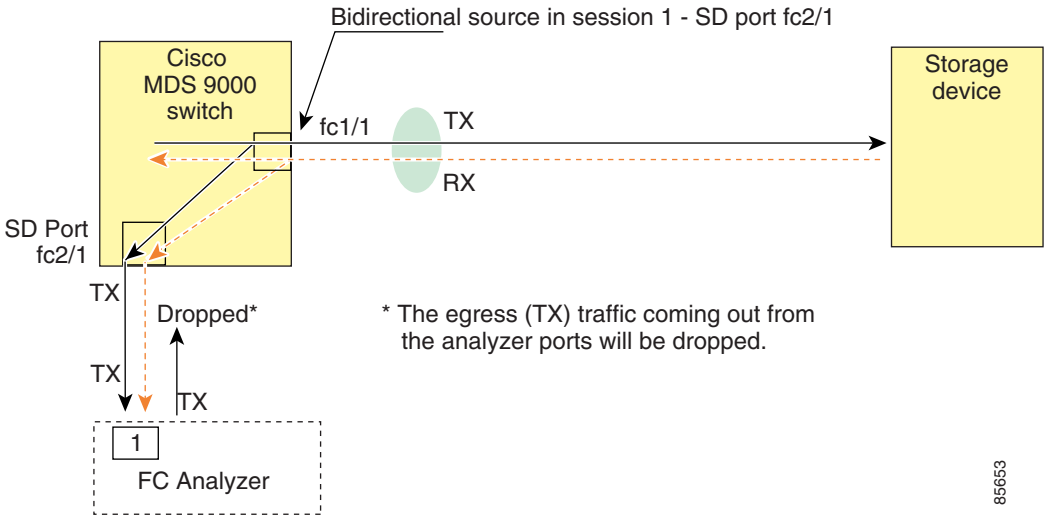
	Command	Purpose
Step 4	`switch(config-span)# source interface fc1/1 rx`	Configures the source interface fc1/1 in the ingress direction.
Step 5	`switch(config)# span session 2` `switch(config-span)#`	Creates the SPAN session 2.
Step 6	`switch(config-span)## destination interface fc2/2`	Configures the destination interface fc2/2.
Step 7	`switch(config-span)# source interface fc1/1 tx`	Configures the source interface fc1/1 in the egress direction.

Single SD Port to Monitor Traffic

You do not need to use two SD ports to monitor bidirectional traffic on any interface as shown in Figure 52-6. You can use one SD port and one FC analyzer port by monitoring traffic on the interface at the same SD port fc2/1.

Figure 52-7 shows a SPAN setup where one session with destination port fc2/1 and source interface fc1/1 is used to capture traffic in both ingress and egress directions. This setup is more advantageous and cost effective than the setup shown in Figure 52-6—it uses one SD port and one port on the analyzer, instead of using a full, two-port analyzer.

Figure 52-7 Fibre Channel Analyzer Using a Single SD Port



To use this setup, the analyzer should have the capability of distinguishing ingress and egress traffic for all captured frames.

To configure SPAN on a single SD port, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# span session 1` `switch(config-span)#`	Creates the SPAN session 1.

	Command	Purpose
Step 3	`switch(config-span)## destination interface fc2/1`	Configures the destination interface fc2/1.
Step 4	`switch(config-span)# source interface fc1/1`	Configures the source interface fc1/1 on the same SD port.

Displaying SPAN Information

Use the **show span** command to display configured SPAN information. See Examples 52-4 to 52-7.

Example 52-4 Displays SPAN Sessions in a Brief Format

```
switch# show span session brief
-------------------------------------------------------
 Session  Admin          Oper           Destination
          State          State          Interface
-------------------------------------------------------
 7        no suspend     active         fc2/7
 1        suspend        inactive       not configured
 2        no suspend     inactive       fc3/1
```

Example 52-5 Displays a Specific SPAN Session in Detail

```
switch# show span session 7
Session 7 (active)
   Destination is fc2/7
   No session filters configured
   No ingress (rx) sources
   Egress (tx) sources are
     port-channel 7,
```

Example 52-6 Displays ALL SPAN Sessions

```
switch# show span session
Session 1 (inactive as no destination)
Destination is not specified
   Session filter vsans are 1
   No ingress (rx) sources
   No egress (tx) sources
Session 2 (active)
   Destination is fc9/5
   No session filters configured
   Ingress (rx) sources are
      vsans 1
   No egress (tx) sources
Session 3 (admin suspended)
   Destination is not configured
   Session filter vsans are 1-20
   Ingress (rx) sources are
     fc3/2, fc3/3, fc3/4, fcip 51,
     port-channel 2, sup-fc0,
   Egress (tx) sources are
     fc3/2, fc3/3, fc3/4, sup-fc0,
```

Example 52-7 Displays an SD Port Interface with Encapsulation Enabled

```
switch# show int fc9/32
fc9/32 is up
    Hardware is Fibre Channel
    Port WWN is 22:20:00:05:30:00:49:5e
    Admin port mode is SD
    Port mode is SD
    Port vsan is 1
    Speed is 1 Gbps
    Receive Buffer Size is 2112
    Encapsulation is eisl <---------- Displays the enabled encapsulation status
    Beacon is turned off
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      0 frames input, 0 bytes, 0 discards
        0 CRC,  0 unknown class
        0 too long, 0 too short
      0 frames output, 0 bytes, 0 discards
      0 input OLS, 0 LRR, 0 NOS, 0 loop inits
      0 output OLS, 0 LRR, 0 NOS, 0 loop inits
```

Remote SPAN

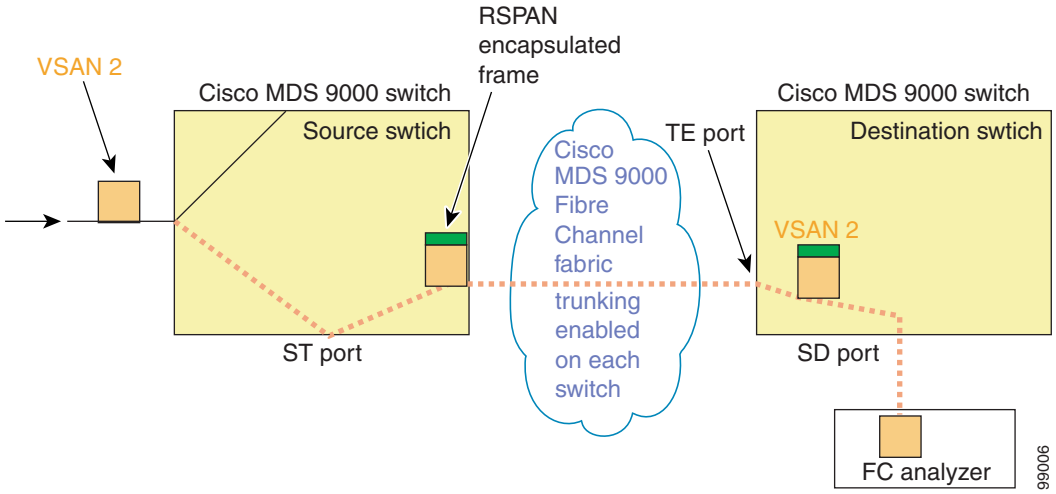
Note Remote SPAN is not supported on the Cisco Fabric Switch for HP c-Class BladeSystem and the Cisco Fabric Switch for IBM BladeSystem.

The Remote SPAN (RSPAN) feature enables you to remotely monitor traffic for one or more SPAN sources distributed in one or more source switches in a Fibre Channel fabric. The SPAN destination (SD) port is used for remote monitoring in a destination switch. A destination switch is usually different from the source switch(es) but is attached to the same Fibre Channel fabric. You can replicate and monitor traffic in any remote Cisco MDS 9000 Family switch or director, just as you would monitor traffic in a Cisco MDS source switch.

The RSPAN feature is nonintrusive and does not affect network traffic switching for those SPAN source ports. Traffic captured on the remote switch is tunneled across a Fibre Channel fabric which has trunking enabled on all switches in the path from the source switch to the destination switch. The Fibre Channel tunnel is structured using trunked ISL (TE) ports. In addition to TE ports, the RSPAN feature uses two other interface types (see Figure 52-8):

- SD ports—A passive port from which remote SPAN traffic can be obtained by the FC analyzer.
- ST ports—A SPAN tunnel (ST) port is an entry point port in the source switch for the RSPAN Fibre Channel tunnel. ST ports are special RSPAN ports and cannot be used for normal Fibre Channel traffic.

Figure 52-8 RSPAN Transmission



Advantages to Using RSPAN

The RSPAN features has the following advantages:

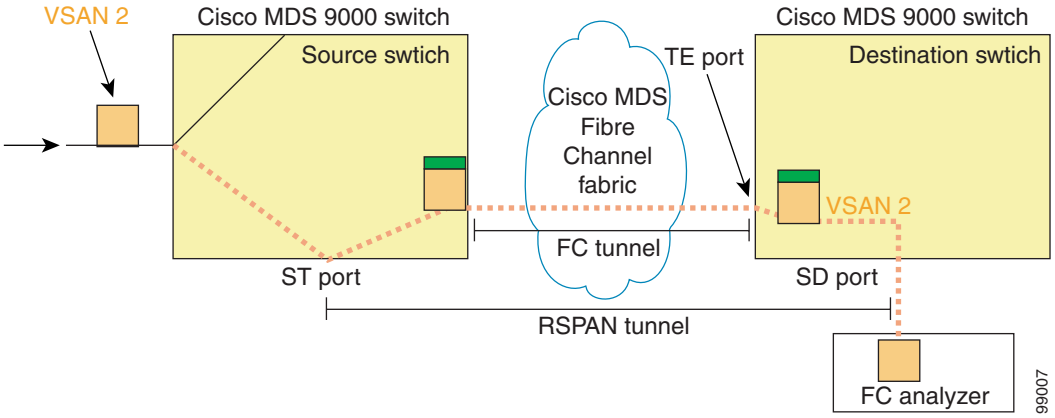
- Enables nondisruptive traffic monitoring at a remote location.
- Provides a cost effective solution by using one SD port to monitor remote traffic on multiple switches.
- Works with any Fibre Channel analyzer.
- Is compatible with the Cisco MDS 9000 Port Analyzer adapters.
- Does not affect traffic in the source switch, but shares the ISL bandwidth with other ports in the fabric.

FC and RSPAN Tunnels

An FC tunnel is a logical data path between a source switch and a destination switch. The FC tunnel originates from the source switch and terminates at the remotely located destination switch.

RSPAN uses a special Fibre Channel tunnel (FC tunnel) that originates at the ST port in the source switch and terminates at the SD port in the destination switch. You must bind the FC tunnel to an ST port in the source switch and map the same FC tunnel to an SD port in the destination switch. Once the mapping and binding is configured, the FC tunnel is referred to as an RSPAN tunnel (see Figure 52-9).

Figure 52-9 FC and RSPAN Tunnel



Guidelines to Configure RSPAN

The following guidelines apply for a SPAN configuration:

- All switches in the end-to-end path of the RSPAN tunnel must belong to the Cisco MDS 9000 Family.
- All VSANs with RSPAN traffic must be enabled. If a VSAN containing RSPAN traffic is not enabled, it is dropped.
- The following configurations must be performed on *each* switch in the end-to-end path of the Fibre Channel tunnel in which RSPAN is to be implemented:
  - Trunking must be enabled (enabled by default).
  - VSAN interface must be configured.
  - The Fibre Channel tunnel feature must be enabled (disabled by default).
  - IP routing must be enabled (disabled by default).

Note If the IP address is in the same subnet as the VSAN, the VSAN interface does not have to be configured for all VSANs on which the traffic is spanned.

- A single Fibre Channel switch port must be dedicated for the ST port functionality.
- Do not configure the port to be monitored as the ST port.
- The FC tunnel's IP address must reside in the same subnet as the VSAN interface

  See Chapter 43, "Configuring IP Services."

ST Port Characteristics

ST ports have the following characteristics:

- ST ports perform the RSPAN encapsulation of the FC frame.
- ST ports do not use BB_credits.
- One ST port can only be bound to one FC tunnel.

- ST ports cannot be used for any purpose other than to carry RSPAN traffic.
- ST ports cannot be configured using Storage Services Modules (SSMs).

Configuring RSPAN

The RSPAN tunnel begins in the source switch and terminates in the destination switch. This section assumes Switch S to be the source and Switch D to be the destination.

Note Besides the source and destination switches, the VSAN must also be configured in each Cisco MDS switch in the Fibre Channel fabric, if they exist.

To monitor network traffic using the RSPAN feature, follow these steps:

Step 1 Create VSAN interfaces in destination switch (Switch D) and source switch (Switch S) to facilitate the Fibre Channel tunnel (FC tunnel) creation.

Step 2 Enable the FC tunnel in each switch in the end-to-end path of the tunnel.

Step 3 Initiate the FC tunnel (in Switch S) and map the tunnel to the VSAN interface's IP address (in Switch D) so all RSPAN traffic from the tunnel is directed to the SD port.

Step 4 Configure SD ports for SPAN monitoring in the destination switch (Switch D).

Step 5 Configure the ST port in the source switch (Switch S) and bind the ST port to the FC tunnel.

Step 6 Create an RSPAN session in the source switch (in Switch S) to monitor network traffic.

RSPAN Configuration Example

This section provides a RSPAN configuration example using the procedure defined in the previous section.

Configuration in the Source Switch

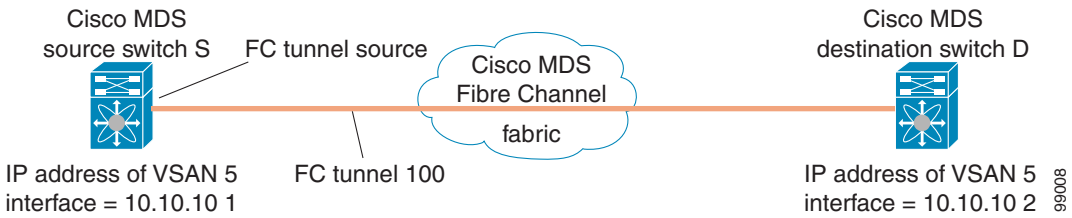
This section identifies the tasks that must be performed in the source switch (Switch S):

- Configuring the SD Port, page 52-23
- Mapping the FC Tunnel, page 52-24

Creating VSAN Interfaces

Figure 52-10 depicts a basic FC tunnel configuration.

Figure 52-10 FC Tunnel Configuration



Note This example assumes that VSAN 5 is already configured in the VSAN database.

To create a VSAN interface in the source switch for the scenario in Figure 52-10, follow these steps:

	Command	Purpose
Step 1	`switchS# config t`	Enters configuration mode.
Step 2	`switchS(config)# interface vsan 5` `switchS(config-if)#`	Configures the specified VSAN interface (VSAN 5) in the source switch (switch S).
Step 3	`switchS(config-if)# ip address 10.10.10.1 255.255.255.0`	Configures the IPv4 address and subnet for the VSAN interface 5 in the source switch (switch S).
Step 4	`switchS(config-if)# no shutdown`	Enables traffic flow through this interface.

Enabling FC Tunnels

To enable the FC tunnel feature, follow these steps:

	Command	Purpose
Step 1	`switchS# config t`	Enters configuration mode.
Step 2	`switchS(config)# fc-tunnel enable`	Enables the FC tunnel feature (disabled by default).

Note Be sure to enable this feature in each switch in the end-to-end path in the fabric.

Initiating the FC Tunnel

To initiate the FC tunnel in the source switch for the scenario in Figure 52-10, follow these steps:

	Command	Purpose
Step 1	`switchS# config t`	Enters configuration mode.
Step 2	`switchS(config)# interface fc-tunnel 100` `switchS(config-if)#`	Initiates the FC tunnel (100) in the source switch (switch S). The tunnel IDs range from 1 to 255.
Step 3	`switchS(config-if)# source 10.10.10.1`	Maps the IPv4 address of the source switch (switch S) to the FC tunnel (100).
Step 4	`switchS(config-if)# destination 10.10.10.2`	Maps the IPv4 address of the destination switch (switch D) to the FC tunnel (100).
Step 5	`switchS(config-if)# no shutdown`	Enables traffic flow through this interface.

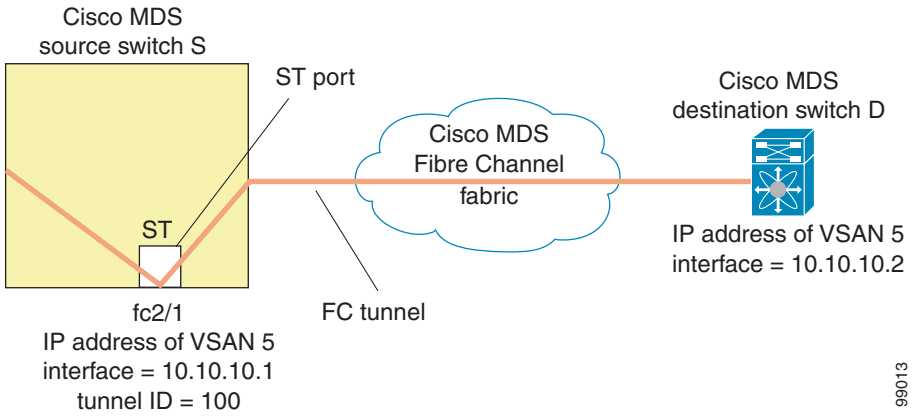
Tip The interface cannot be operationally up until the FC tunnel mapping is configured in the destination switch.

Configuring the ST Port

Once the FC tunnel is created, be sure to configure the ST port to bind it to the FC tunnel at the source switch. The FC tunnel becomes an RSPAN tunnel once the binding and mapping is complete.

Figure 52-11 depicts a basic FC tunnel configuration.

Figure 52-11 Binding the FC Tunnel



Note ST ports cannot be configured using Storage Services Modules (SSMs).

To configure an ST port for the scenario in Figure 52-11, follow these steps:

	Command	Purpose
Step 1	`switchS# config t`	Enters configuration mode.
Step 2	`switchS(config)# interface fc2/1`	Configures the specified interface.

	Command	Purpose
Step 3	`switchS(config-if)# switchport mode ST`	Configures the ST port mode for interface fc2/1.
Step 4	`switchS(config-if)# switchport speed 2000`	Configures the ST port speed to 2000 Mbps.
Step 5	`switchS(config-if)# rspan-tunnel interface fc-tunnel 100`	Associates and binds the ST port with the RSPAN tunnel (100).
Step 6	`switchS(config-if)# no shutdown`	Enables traffic flow through this interface.

Configuring an RSPAN Session

A RSPAN session is similar to a SPAN session, with the destination interface being an RSPAN tunnel.

To configure an RSPAN session in the source switch for the scenario in Figure 52-11, follow these steps:

	Command	Purpose
Step 1	`switchS# config t`	Enters configuration mode.
Step 2	`switchS(config)# span session 2` `switchS(config-span)#`	Configures the specified SPAN session (2). If the session does not exist, it is created. The session ID ranges from 1 to 16.
Step 3	`switchS(config-span)# destination interface fc-tunnel 100`	Configures the specified RSPAN tunnel (100) in a session.
Step 4	`switchS(config-span)# source interface fc1/1`	Configures the source interface (fc1/1) for this session and spans the traffic from interface fc1/1 to RSPAN tunnel 100.

Configuration in All Intermediate Switches

This section identifies the tasks that must be performed in all intermediate switches in the end-to-end path of the RSPAN tunnel:

- Configuring VSAN Interfaces, page 52-21
- Enabling FC Tunnels, page 52-22
- Enabling IP Routing, page 52-22

Configuring VSAN Interfaces

Figure 52-12 on page 52-23 depicts an RSPAN tunnel configuration terminating in the destination switch (Switch D).

Note This example assumes that VSAN 5 is already configured in the VSAN database.

To create a VSAN interface in the destination switch for the scenario in Figure 52-12 on page 52-23, follow these steps:

	Command	Purpose
Step 1	`switchD# config t`	Enters configuration mode.
Step 2	`switchD(config)# interface vsan 5` `switchD(config-if)#`	Configures the specified VSAN interface (VSAN 5) in the destination switch (Switch D).

	Command	Purpose
Step 3	`switchD(config-if)# ip address 10.10.10.2 255.255.255.0`	Configures the IPv4 address and subnet for the VSAN interface in the destination switch (Switch D).
Step 4	`switchD(config-if)# no shutdown`	Enables traffic flow to administratively allow traffic (provided the operational state is up).

Enabling FC Tunnels

To enable the FC tunnel feature, follow these steps:

	Command	Purpose
Step 1	`switchS# config t`	Enters configuration mode.
Step 2	`switchS(config)# fc-tunnel enable`	Initiates the FC tunnel (100) in the source switch (switch S). The tunnel IDs range from 1 to 255.

Note Be sure to enable this feature in each switch in the end-to-end path in the fabric.

Enabling IP Routing

The IP routing feature is disabled by default. Be sure to enable IP routing in each switch (including the source and destination switches) in the end-to-end path in the fabric (see the "Enabling IPv4 Routing" section on page 43-7). This step is required to set up the FC tunnel.

Configuration in the Destination Switch

This section identifies the tasks that must be performed in the destination switch (Switch D):

- Configuring VSAN Interfaces, page 52-22
- Configuring the SD Port, page 52-23
- Mapping the FC Tunnel, page 52-24

Configuring VSAN Interfaces

Figure 52-12 on page 52-23 depicts an RSPAN tunnel configuration terminating in the destination switch (Switch D).

Note This example assumes that VSAN 5 is already configured in the VSAN database.

To create a VSAN interface in the destination switch for the scenario in Figure 52-12, follow these steps:

	Command	Purpose
Step 1	`switchD# config t`	Enters configuration mode.
Step 2	`switchD(config)# interface vsan 5` `switchD(config-if)#`	Configures the specified VSAN interface (VSAN 5) in the destination switch (Switch D).

	Command	Purpose
Step 3	`switchD(config-if)# ip address 10.10.10.2 255.255.255.0`	Configures the IPv4 address and subnet for the VSAN interface in the destination switch (Switch D).
Step 4	`switchD(config-if)# no shutdown`	Enables traffic flow to administratively allow traffic (provided the operational state is up).

Enabling FC Tunnels

To enable the FC tunnel feature, follow these steps:

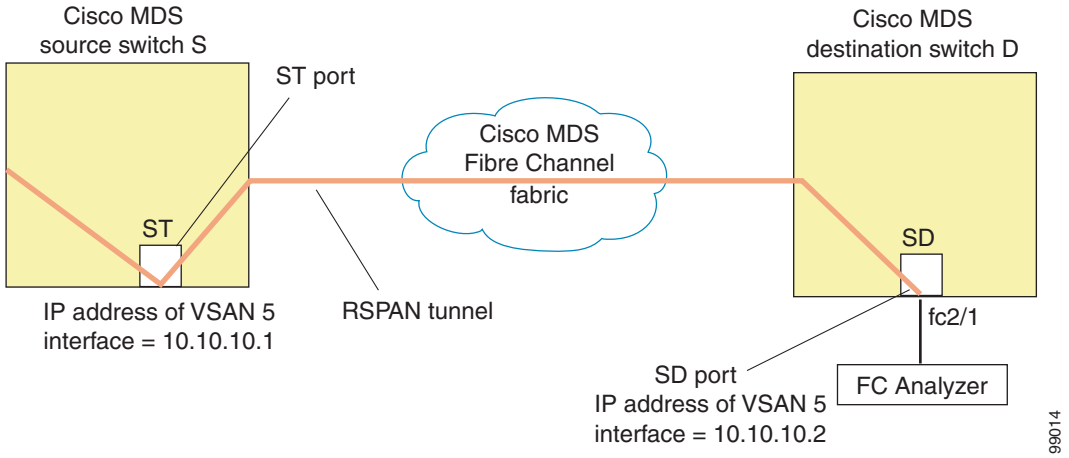
	Command	Purpose
Step 1	`switchS# config t`	Enters configuration mode.
Step 2	`switchS(config)# fc-tunnel enable`	Initiates the FC tunnel (100) in the source switch (switch S). The tunnel IDs range from 1 to 255.

Note Be sure to enable this feature in each switch in the end-to-end path in the tunnel.

Configuring the SD Port

The SD port in the destination switch enables the FC analyzer to receive the RSPAN traffic from the Fibre Channel tunnel. Figure 52-12 depicts an RSPAN tunnel configuration, now that tunnel destination is also configured.

Figure 52-12 RSPAN Tunnel Configuration



Note SD ports cannot be configured using Storage Services Modules (SSMs).

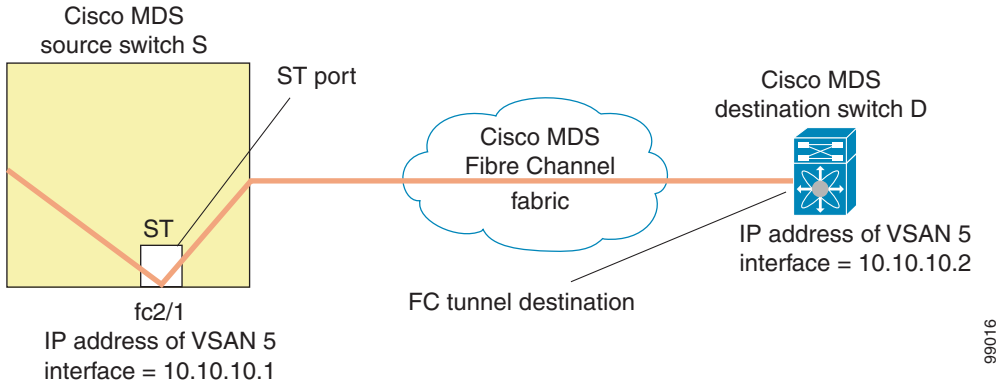
To configure an SD port for the scenario in Figure 52-12, follow these steps:

	Command	Purpose
Step 1	`switchD# config t`	Enters configuration mode.
Step 2	`switchD(config)# interface fc2/1`	Configures the specified interface.
Step 3	`switchD(config-if)# switchport mode SD`	Configures the SD port mode for interface fc2/1.
Step 4	`switchD(config-if)# switchport speed 2000`	Configures the SD port speed to 2000 Mbps.
Step 5	`switchD(config-if)# no shutdown`	Enables traffic flow through this interface.

Mapping the FC Tunnel

The **tunnel-id-map** option specifies the egress interface of the tunnel at the destination switch (see Figure 52-13).

Figure 52-13 FC Tunnel Configuration



To terminate the FC tunnel in the destination switch for the scenario in Figure 52-13, follow these steps:

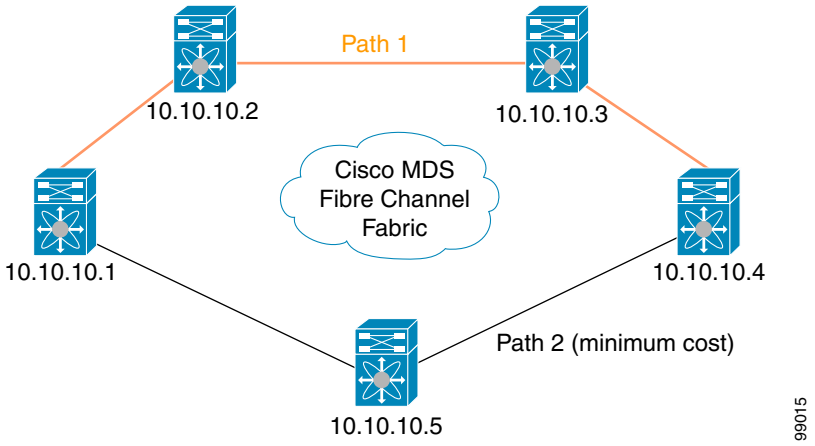
	Command	Purpose
Step 1	`switchD# config t`	Enters configuration mode.
Step 2	`switchD(config)# fc-tunnel tunnel-id-map 100 interface fc2/1`	Terminates the FC tunnel (100) in the destination switch (switch D). The tunnel ID range is from 1 to 255.

Explicit Paths

You can specify an explicit path through the Cisco MDS Fibre Channel fabric (source-based routing), using the **explicit-path** option. For example, if you have multiple paths to a tunnel destination, you can use this option to specify the FC tunnel to always take one path to the destination switch. The software then uses this specified path even if other paths are available.

This option is especially useful if you prefer to direct the traffic through a certain path although other paths are available. In an RSPAN situation, you can specify the explicit path so the RSPAN traffic does not interfere with the existing user traffic. You can create any number of explicit paths in a switch (see Figure 52-14).

Figure 52-14 Explicit Path Configuration



The explicit path must be created in the source switch. To configure an explicit path, you must first create the path and then configure the use of any one path. If an explicit path is not configured, the minimum cost path is used by default. If an explicit path is configured and is functioning, the specified path is used.

To create an explicit path for the scenario in Figure 52-14, follow these steps:

	Command	Purpose
Step 1	`switchS# config t`	Enters configuration mode.
Step 2	`switchS(config)# fc-tunnel explicit-path Path1` `switch(config-explicit-path)#`	Places you at the explicit path prompt for the path named Path 1.

Step 3	`switchS(config-explicit-path)# next-address 10.10.10.2 strict`
	`switchS(config-explicit-path)# next-address 10.10.10.3 strict`
	`switchS(config-explicit-path)# next-address 10.10.10.4 strict`
		Specifies that the next hop VSAN interface IPv4 addresses and the previous hops specified in the explicit path do not require direct connection.

Step 4	`switchS(config)# fc-tunnel explicit-path Path2` `switch(config-explicit-path)#`	Places you at the explicit path prompt for Path2.
Step 5	`switchS(config-explicit-path)# next-address 10.10.10.5 strict` `switchS(config-explicit-path)# next-address 10.10.10.4 strict`	Specifies that the next hop VSAN interface IPv4 addresses and the previous hops specified in the explicit path do not require direct connection.
Step 6	`switchS(config)# fc-tunnel explicit-path Path3` `switch(config-explicit-path)#`	Places you at the explicit path prompt for Path3.
Step 7	`switchS(config-explicit-path)# next-address 10.10.10.3 loose`	Configures a minimum cost path in which the 10.10.10.3 IPv4 address exists. **Note** In Figure 52-14, Path 3 is the same as Path 1—10.10.10.3 exists in Path 1. Using the **loose** option, you can achieve the same effect with one command instead of issuing three commands (using the **strict** option) in Step 3.

To reference the explicit path, follow these steps:

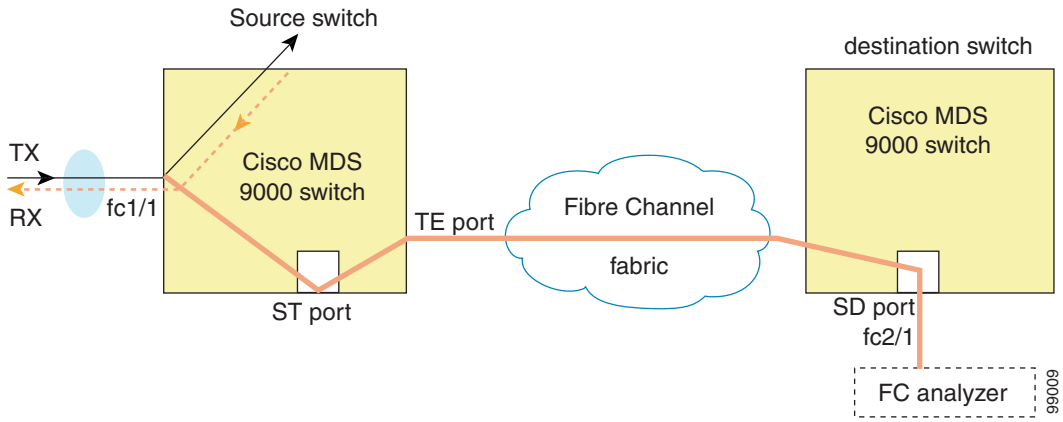
	Command	Purpose
Step 1	`switchS# config t`	Enters configuration mode.
Step 2	`switchS(config)# interface fc-tunnel 100`	References the tunnel ID for Path1.
Step 3	`switchS(config)# explicit-path Path1`	Links Path1 to the tunnel ID.

This configuration explicitly specifies Path 1 to be used for the RSPAN traffic. Refer to RFC 3209 for further details on explicit paths and source based routing.

Monitoring RSPAN Traffic

Once the session is configured, other SPAN sources for this session can also be configured as required. Figure 52-15 shows an RSPAN setup where one session with destination port fc2/1 and source interface fc1/1 is used to capture traffic in both ingress and egress directions.

Figure 52-15 Fibre Channel Analyzer Using a Single SD Port to Monitor RSPAN Traffic



To use this setup, the analyzer should have the capability of distinguishing ingress and egress traffic for all captured frames.

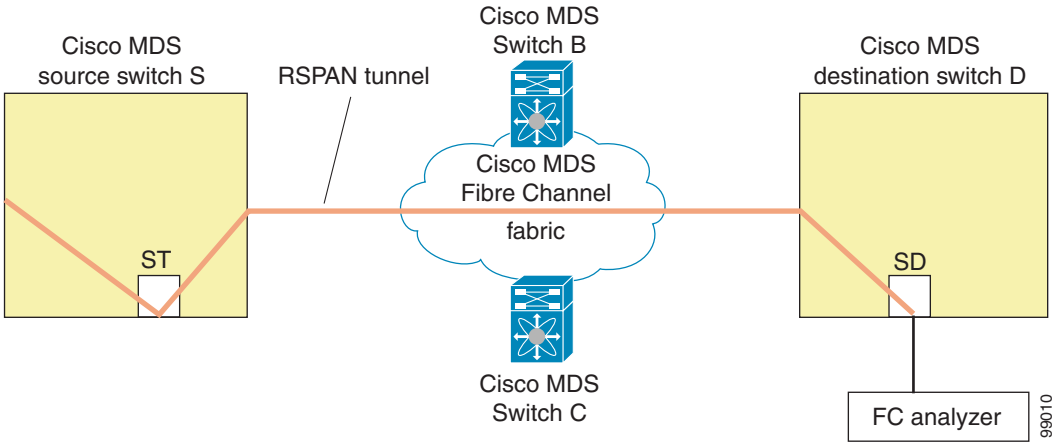
Sample Scenarios

Note RSPAN can be combined with the local SPAN feature so SD ports forward local SPAN traffic along with remote SPAN traffic. Various SPAN source and tunnel scenarios are described in this section.

Single Source with One RSPAN Tunnel

The source Switch S and the destination Switch D are interconnected through a Fibre Channel fabric. An RSPAN tunnel is configured as a destination interface for the SPAN session and the ST port forwards SPAN traffic through the RSPAN tunnel (see Figure 52-16).

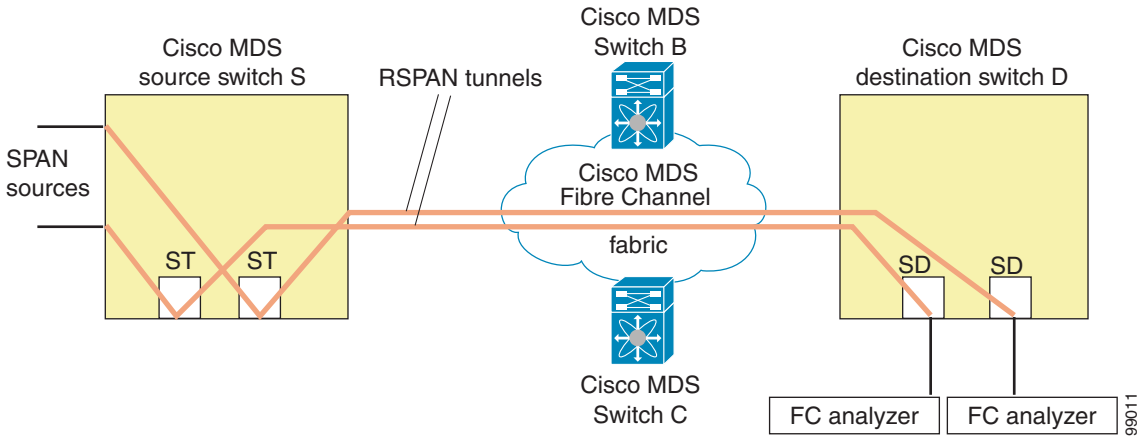
Figure 52-16 RSPAN Scenario with One Source Switch, One Destination Switch, and One Tunnel



Single Source with Multiple RSPAN Tunnels

Figure 52-17 displays two separate RSPAN tunnels configured between Switches S and N. Each tunnel has an associated ST port in the source switch and a separate SD port in the destination switch. This configuration is useful for troubleshooting purposes.

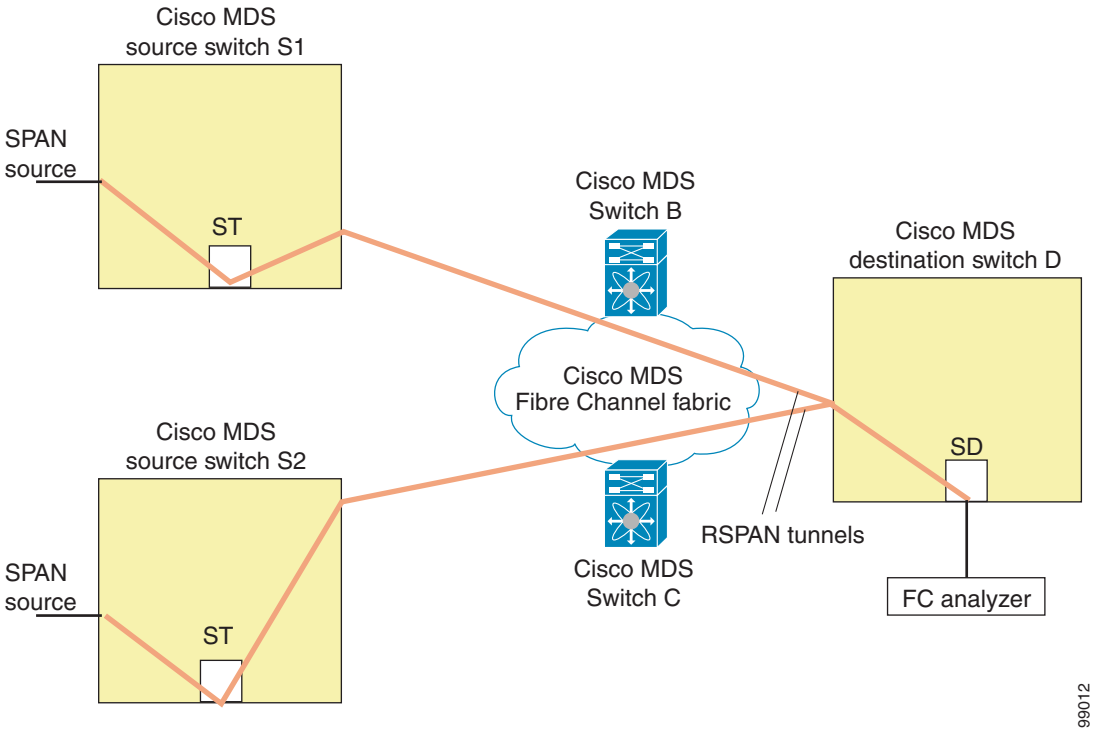
Figure 52-17 RSPAN Scenario with One Source Switch, One Destination Switch, and Multiple Tunnels



Multiple Sources with Multiple RSPAN Tunnels

Figure 52-18 displays two separate RSPAN tunnels configured between Switches S1 and S2. Both tunnels have an associated ST port in their respective source switch and terminate in the same SD port in the destination switch.

Figure 52-18 RSPAN Scenario with Two Source Switches, a Destination Switch, and Multiple Tunnels



This configuration is useful for remote monitoring purposes. For example, the administrator may be at the destination switch and can remotely monitor the two source switches.

Displaying RSPAN Information

Use the **show** commands to display configured RSPAN information. See Examples 52-8 to 52-14.

Example 52-8 Displays ST Port Interface Information

```
switch# show interface brief

--------------------------------------------------------------------------------
Interface   Vsan    Admin    Admin    Status      Oper    Oper    Port-channel
                    Mode     Trunk                Mode    Speed
                             Mode                         (Gbps)
--------------------------------------------------------------------------------
fc1/1       1       auto     on       trunking    TE          2       --
...
fc1/14      1       auto     on       trunking    TE          2       --
fc1/15      1       ST       on       up          ST          2       --
...
fc2/9       1       auto     on       trunking    TE          2       port-channel 21
fc2/10      1       auto     on       trunking    TE          2       port-channel 21
...
fc2/13      999     auto     on       up          F           1       --
fc2/14      999     auto     on       up          FL          1       --
fc2/15      1       SD       --       up          SD          2       --
fc2/16      1       auto     on       trunking    TE          2       --
```

```
--------------------------------------------------------------------------------
Interface           Status      Speed
                                (Gbps)
--------------------------------------------------------------------------------
sup-fc0             up          1

--------------------------------------------------------------------------------
Interface           Status      IP Address              Speed       MTU
--------------------------------------------------------------------------------
mgmt0               up          172.22.36.175/22        100 Mbps    1500

--------------------------------------------------------------------------------
Interface           Status      IP Address              Speed       MTU--
--------------------------------------------------------------------------------
vsan5               up          10.10.10.1/24           1 Gbps      1500
--------------------------------------------------------------------------------
Interface           Vsan        Admin           Status      Oper    Oper
                                Trunk                       Mode    Speed
                                Mode                                (Gbps)
--------------------------------------------------------------------------------
port-channel 21     1           on              trunking    TE      4
--------------------------------------------------------------------------------
Interface           Status      Dest IP Addr    Src IP Addr     TID    Explicit Path
--------------------------------------------------------------------------------
fc-tunnel 100       up          10.10.10.2      10.10.10.1      100
```

Example 52-9 Displays Detailed Information for the ST Port Interface

```
switch# show interface fc1/11
fc1/11 is up
    Hardware is Fibre Channel
    Port WWN is 20:0b:00:05:30:00:59:de
    Admin port mode is ST
    Port mode is ST
    Port vsan is 1
    Speed is 1 Gbps
    Rspan tunnel is fc-tunnel 100
    Beacon is turned off
    5 minutes input rate 248 bits/sec, 31 bytes/sec, 0 frames/sec
    5 minutes output rate 176 bits/sec, 22 bytes/sec, 0 frames/sec
      6862 frames input, 444232 bytes
        0 discards, 0 errors
        0 CRC, 0 unknown class
        0 too long, 0 too short
      6862 frames output, 307072 bytes
        0 discards, 0 errors
      0 input OLS, 0 LRR, 0 NOS, 0 loop inits
      0 output OLS, 0 LRR, 0 NOS, 0 loop inits
```

Example 52-10 Displays the FC Tunnel Status

```
switch# show fc-tunnel
fc-tunnel is enabled
```

Example 52-11 Displays FC Tunnel Egress Mapping Information

```
switch# show fc-tunnel tunnel-id-map
tunnel id egress interface
    150     fc3/1
    100     fc3/1
```

Note Multiple tunnel IDs can terminate at the same interface.

Example 52-12 Displays FC Tunnel Explicit Mapping Information

```
switch# show fc-tunnel explicit-path
Explicit path name: Alternate1
       10.20.1.2 loose
       10.20.1.3 strict
Explicit path name: User2
       10.20.50.1 strict
       10.20.50.4 loose
```

Example 52-13 Displays SPAN Mapping Information

```
switch# show span session
Session 2 (active)
   Destination is fc-tunnel 100
   No session filters configured
   Ingress (rx) sources are
     fc2/16,
   Egress (tx) sources are
     fc2/16,
```

Example 52-14 Displays the FC Tunnel Interface

```
switch# show interface fc-tunnel 200
fc-tunnel 200 is up
Dest   IP Addr: 200.200.200.7   Tunnel ID: 200
Source IP Addr: 200.200.200.4   LSP ID: 1
Explicit Path Name:
```

Default SPAN and RSPAN Settings

Table 52-1 lists the default settings for SPAN parameters.

Table 52-1 Default SPAN Configuration Parameters

Parameters	Default
SPAN session	Active.
If filters are not specified	SPAN traffic includes traffic through a specific interface from all active VSANs.
Encapsulation	Disabled.
SD port	Output frame format is Fibre Channel.

Table 52-2 lists the default settings for RSPAN parameters.

Table 52-2 Default RSPAN Configuration Parameters

Parameters	Default
FC tunnel	Disabled.
Explicit path	Not configured.
Minimum cost path	Used if explicit path is not configured.