Monitoring Network Traffic Using SPAN

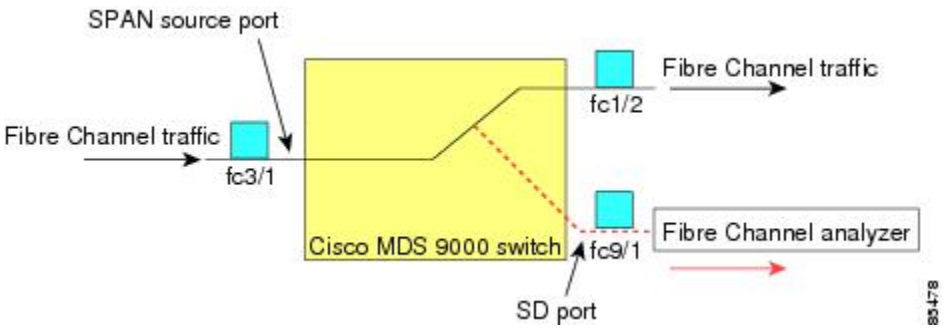
This chapter describes the Switched Port Analyzer (SPAN) features provided in switches in the Cisco MDS 9000 Family.

Information 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.

SD ports do not receive frames, they only transmit a copy of the SPAN source traffic. The SPAN feature is nonintrusive and does not affect switching of network traffic for any SPAN source ports (see Figure 1: SPAN Transmission, on page 1).

Figure 1: SPAN Transmission

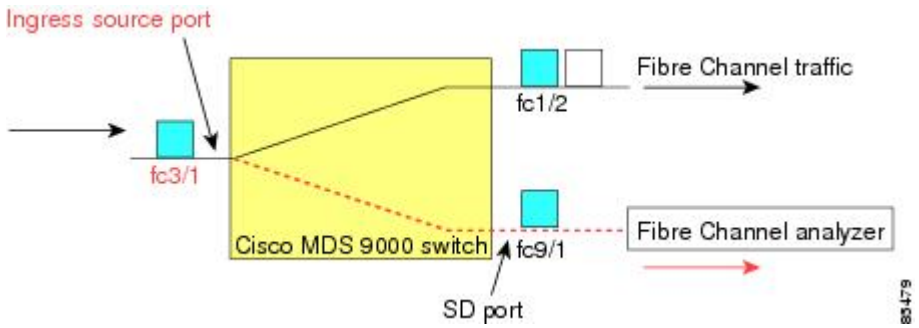


SPAN Sources

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. When a VSAN as a source is specified, then all physical ports and PortChannels in that 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:

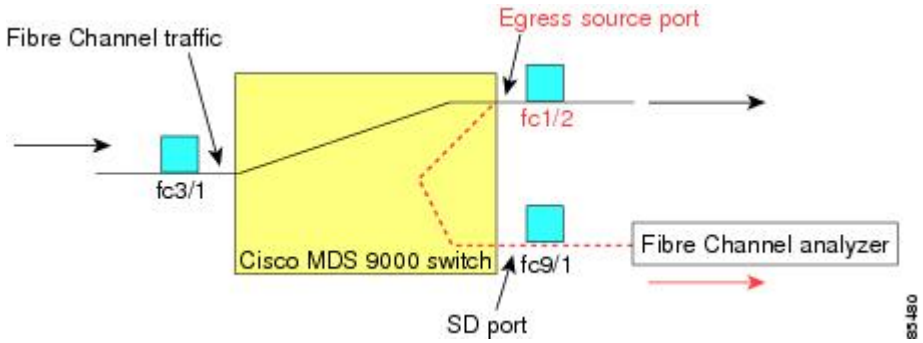
- Ingress source (Rx)—Traffic entering the switch fabric through this source interface is *spanned* or copied to the SD port (see Figure 2: SPAN Traffic from the Ingress Direction, on page 2).

Figure 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 3: SPAN Traffic from Egress Direction, on page 2).

Figure 3: SPAN Traffic from Egress Direction



IPS Source Ports

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

Note

- You can configure SPAN for Ethernet traffic using Cisco switches or routers that are connected to the Cisco MDS 9000 Series IPS modules.
- Cisco MDS 9200i switch does not support iSCSI.

From Cisco MDS NX-OS Release 8.5(1), traffic that is sent to a Fibre Channel port that is configured as an SD port can be spanned from FCIP interfaces.

The following are the restrictions for using SPAN for ingress or egress traffic that is sent to a Fibre Channel port that is configured as an SD port can be spanned from FCIP interfaces:

- Only one FCIP interface can be added as the ingress SPAN source.
- FCIP port channel cannot be added as the ingress SPAN source. However, individual FCIP member links can be added as the ingress SPAN source.
- Either the ingress or egress SPAN source can be added in a SPAN session, but not bidirectional. To do a bidirectional SPAN, configure two SPAN sessions, one for ingress and the other for egress, to the same destination SD ports.
- You cannot configure Fibre Channel and FCIP interfaces together as ingress or egress source.

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

Note In Cisco MDS 9700 Series Switches, iSCSI ports are not applicable for the Allowed Source Interface Types.

VSAN as a Source

SPAN sources refer to the interfaces from which traffic can be monitored. 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.

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.

Note On a Cisco MDS 9250i Multiservice Fabric switch, packet drops will occur if the SPAN port cannot keep up with incoming frame bursts. To avoid these packet drops, the speed of the SPAN destination port should be equal to the maximum speed of the source ports. However, when the source is an FCIP interface, the speed of the SPAN destination port should be more than 10G because the FCIP interface is running over a 10G Ethernet physical interface.

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). 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. 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.

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.
- In Cisco MDS 9700 Series Switches, the SD Port supports only 2 Gbps, 4 Gbps, 8 Gbps, and 16 Gbps speeds. The auto speed option is not allowed

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,
```

For Cisco MDS 9700 Series Switches:

```
switch(config-if)# monitor session 1
switch(config-monitor)# source interface fc5/1
switch(config-monitor)# destination interface fc2/9
switch(config-monitor)# no shut
```

```
switch(config-monitor)# show monitor session all
session 1
---------------
ssn direction : both
state : up
source intf :
rx : fc5/1
tx : fc5/1
both : fc5/1
source VLANs :
rx :
tx :
both :
source exception :
rate-limit : Auto
filter VLANs : filter not specified
destination ports : fc2/9
```

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

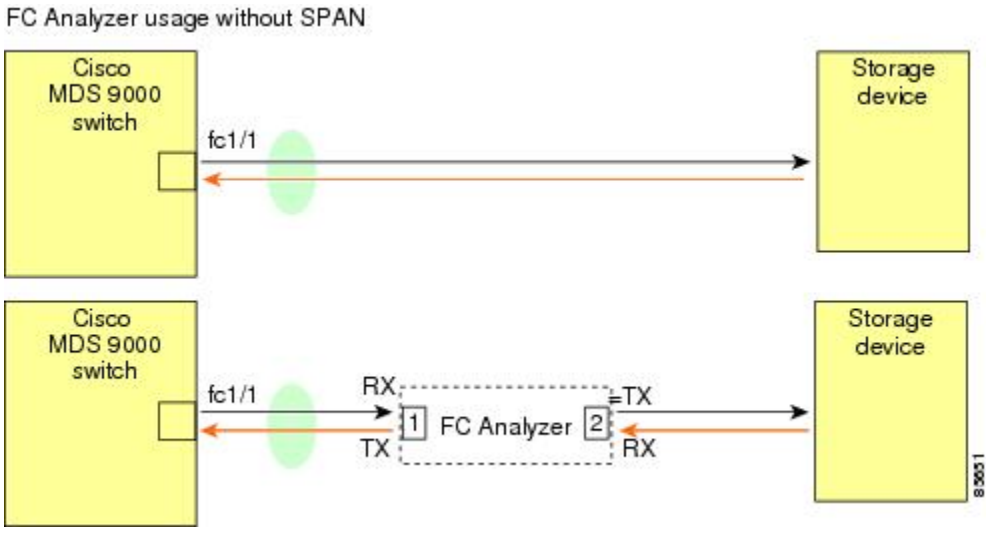
You can use SPAN to monitor traffic on an interface without any traffic disruption. This feature is especially useful in troubleshooting scenarios in which traffic disruption changes the problem environment and makes it difficult to reproduce the problem. You can monitor traffic in either of the following two ways:

- Without SPAN
- With SPAN

Monitoring 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 (see Figure 4: Fibre Channel Analyzer Usage Without SPAN, on page 7).

Figure 4: Fibre Channel Analyzer Usage Without SPAN



This type of connection has the following limitations:

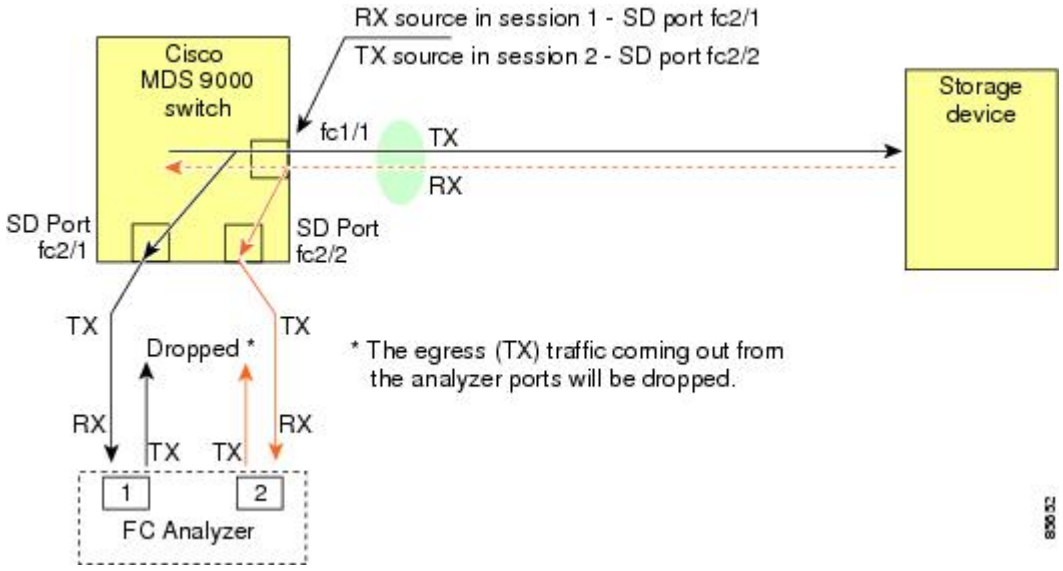
- It requires you to physically insert the FC analyzer between the two network devices.
- It disrupts traffic when the Fibre Channel analyzer is physically connected.
- The analyzer captures data only on the Rx links in both port 1 and port 2. Port 1 captures traffic exiting interface fc1/1 and port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

Monitoring with SPAN

Using SPAN you can capture the same traffic scenario (see Figure 4: Fibre Channel Analyzer Usage Without SPAN, on page 7) 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 (see Figure 5: Fibre Channel Analyzer Using SPAN, on page 8).

Figure 5: Fibre Channel Analyzer Using SPAN

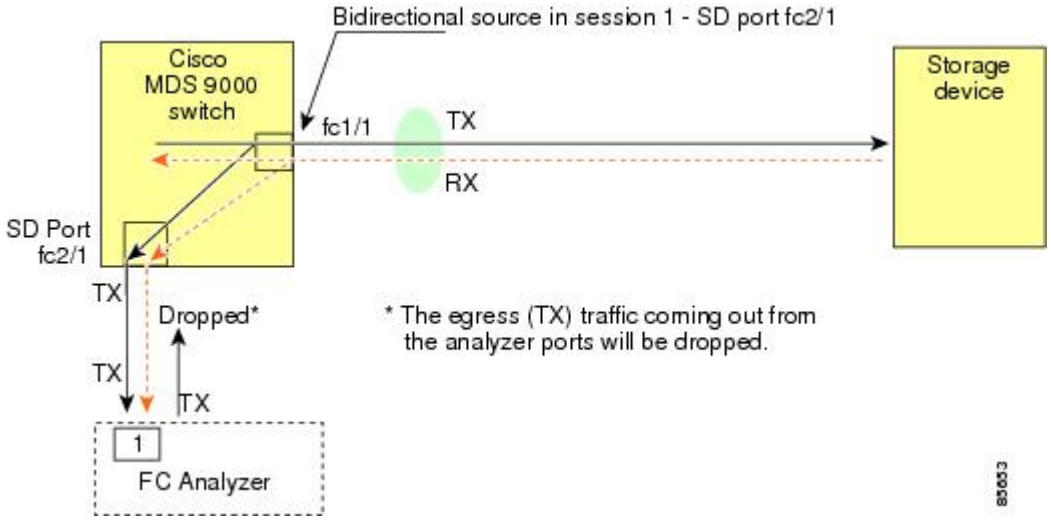


Single SD Port to Monitor Traffic

You do not need to use two SD ports to monitor bidirectional traffic on any interface (see Figure 5: Fibre Channel Analyzer Using SPAN, on page 8). 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 6: Fibre Channel Analyzer Using a Single SD Port, on page 8 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 5: Fibre Channel Analyzer Using SPAN, on page 8. It uses one SD port and one port on the analyzer, instead of using a full, two-port analyzer.

Figure 6: Fibre Channel Analyzer Using a Single SD Port

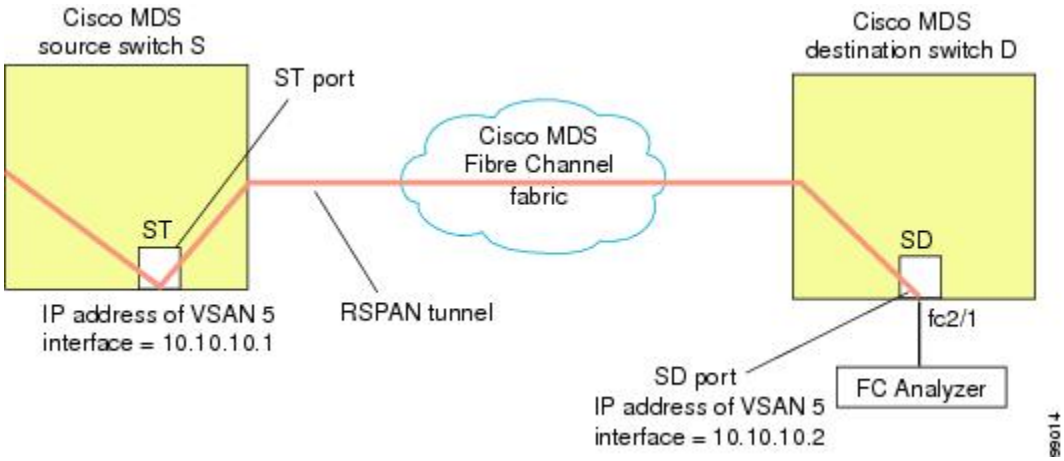


To use this setup, the analyzer should have the capability of distinguishing ingress and egress traffic for all captured frames.

SD Port Configuration

The SD port in the destination switch enables the FC analyzer to receive the RSPAN traffic from the Fibre Channel tunnel. Figure 7: RSPAN Tunnel Configuration, on page 9 depicts an RSPAN tunnel configuration, now that tunnel destination is also configured.

Figure 7: RSPAN Tunnel Configuration

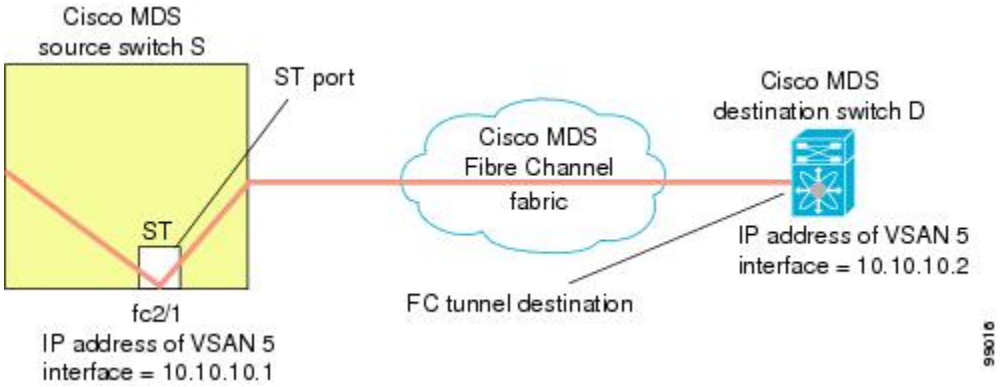


Note SD ports cannot be configured using Storage Services Modules (SSMs).

Mapping the FC Tunnel

The **tunnel-id-map** option specifies the egress interface of the tunnel at the destination switch (see Figure 8: FC Tunnel Configuration, on page 9).

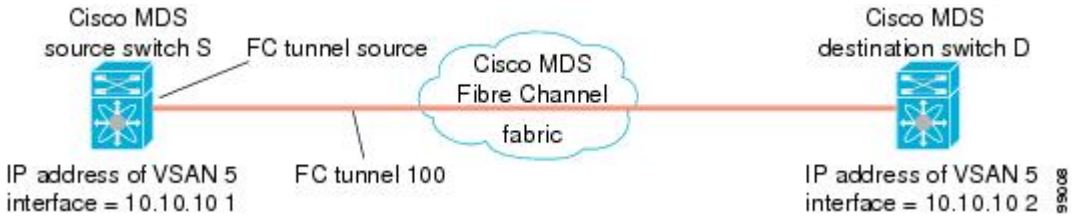
Figure 8: FC Tunnel Configuration



Creating VSAN Interfaces

Figure 9: FC Tunnel Configuration, on page 10 depicts a basic FC tunnel configuration.

Figure 9: FC Tunnel Configuration



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

Remote SPAN

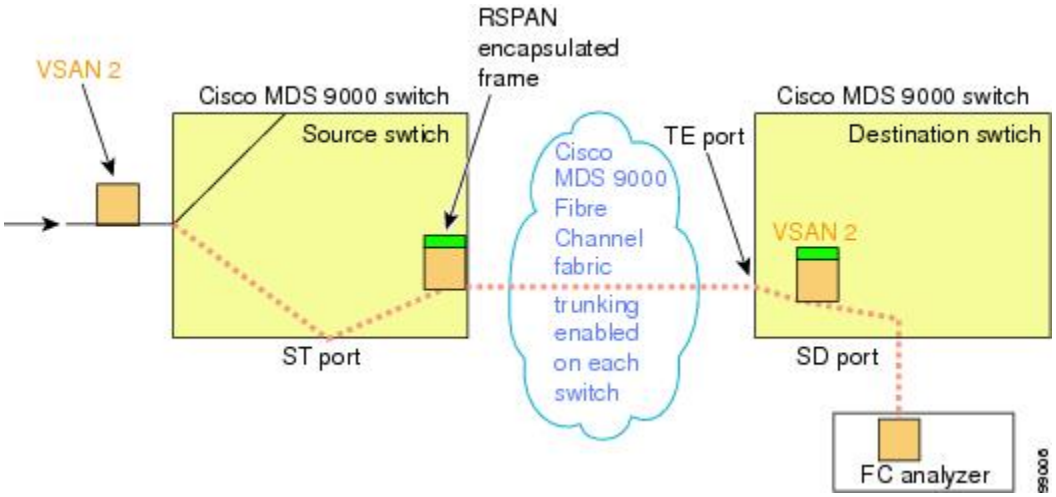
Note Remote SPAN is not supported on the Cisco Fabric Switch for HP c-Class BladeSystem, Cisco Fabric Switch for IBM BladeSystem, Cisco Fabric Switch 9250i, and Cisco Fabric Switch 9100S.

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 10: RSPAN Transmission, on page 11):

- 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 10: RSPAN Transmission



Advantages of Using RSPAN

The RSPAN features has the following advantages:

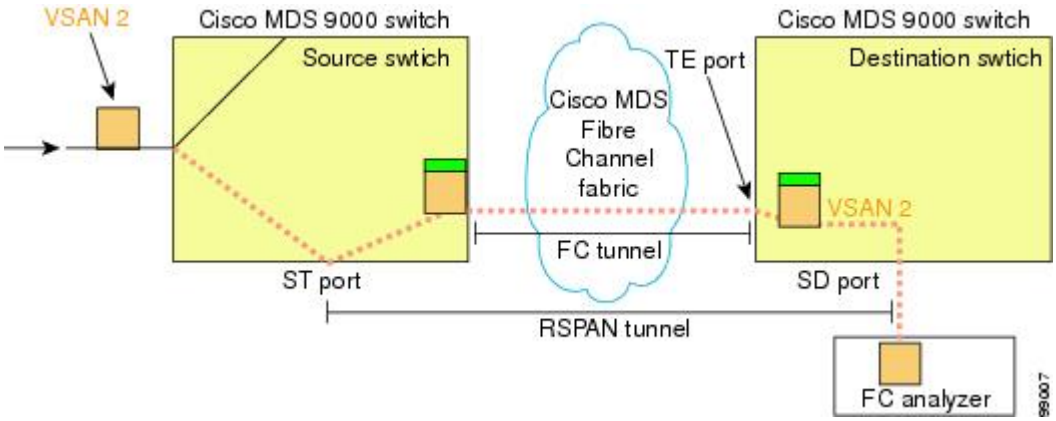
- Enables nondisruptive traffic monitoring at a remote location.
- Provides a cost effective solution by using one SD port to monitor remote traffic on multiple switches.
- Works with any Fibre Channel analyzer.
- Is compatible with the Cisco MDS 9000 Port Analyzer adapters.
- Does not affect traffic 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 11: FC and RSPAN Tunnel, on page 12).

Figure 11: FC and RSPAN Tunnel



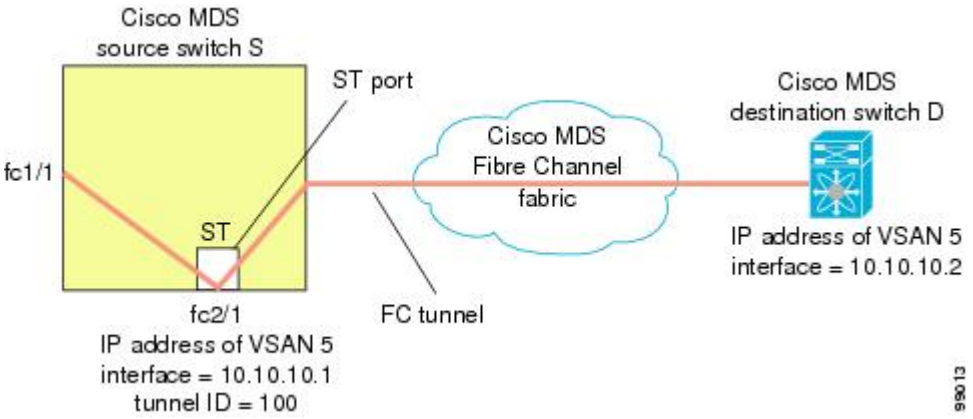
ST Port Configuration

Note In Cisco MDS 9700 Series Switches, SPAN tunnel port (ST port) is not supported.

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 12: Binding the FC Tunnel, on page 12 depicts a basic FC tunnel configuration.

Figure 12: Binding the FC Tunnel



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.

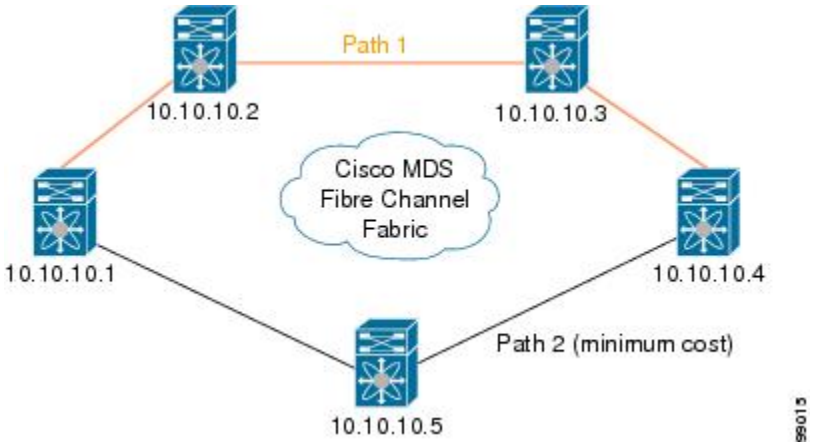
- ST ports cannot be configured using Storage Services Modules (SSMs).

Creating 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 13: Explicit Path Configuration, on page 13).

Figure 13: Explicit Path Configuration



Guidelines and Limitations

Cisco MDS 9700 Series Switches Guidelines

The following guidelines and limitations apply for Cisco MDS 9700 Series Switches:

- In Cisco MDS 9700 Series Switches, SPAN is replaced by Monitor.
- In Cisco MDS 9700 Series Switches, SPAN tunnel port (ST port) is not supported.
- In Cisco MDS 9700 Series Switches, RSPAN is replaced by Remote Monitor.
- For Cisco MDS 9700 Series Switches, Generation 2 Fabric Switches is not supported

SPAN Configuration Guidelines

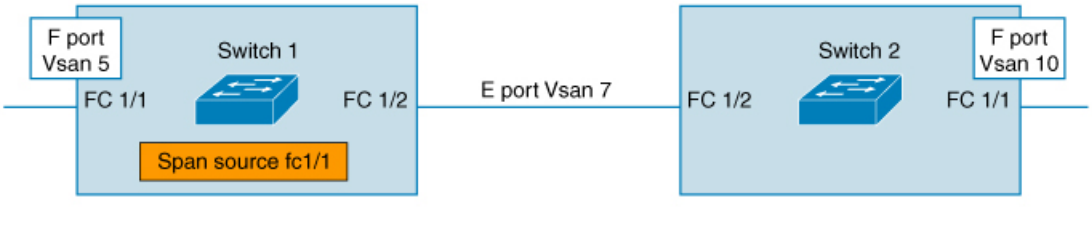
The following guidelines and limitations apply for SPAN configurations:

- You can configure up to 16 SPAN sessions with multiple ingress (Rx) sources.

- The number of source ports must be less than or equal to 16. However, we recommend that you configure a maximum of only two source ports per SPAN or monitor session.
- 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.

Note This is not applicable for Cisco MDS 9700 Series Switches.

- 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.
- SPAN does not capture pause frames in a Fibre Channel over Ethernet (FCoE) network because pause frames sent from the virtual expansion (VE) port are generated and terminated by the outermost MAC layer. For more information on FCoE, see the Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500.
- In case of an IVR configuration and topology, SPAN cannot capture the egress (Tx) of the source port. To span the complete traffic flow, add the source ports taking part in the flow in ingress (Rx) direction.



Consider FC1/1, in the above illustration, as the SPAN source port. In this case, traffic egressing (Tx) from FC1/1 will not be spanned. Only packets entering (Rx) FC1/1 will be spanned. To capture the complete flow, span FC1/1 (Rx) and FC1/2 (Rx) in a single session going to a single destination.

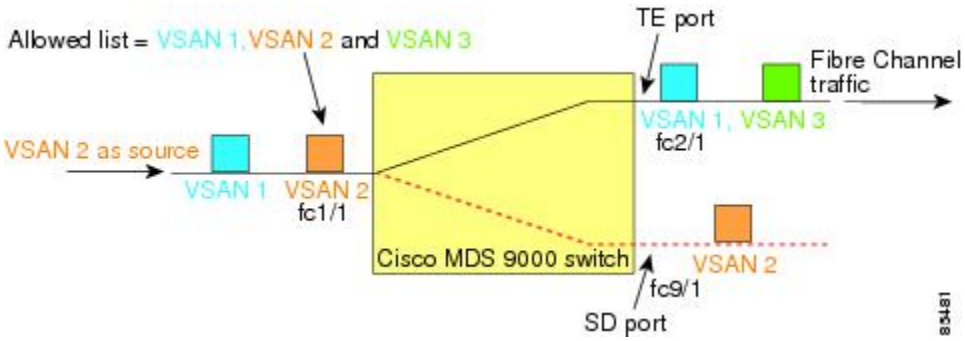
Guidelines to Configure VSANs as a Source

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 14: VSAN as a Source, on page 15 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 14: 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.

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.

RSPAN Configuration Guidelines

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) and the trunk enabled link must be the lowest cost link in the path.
  - 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.

Default SPAN and RSPAN Settings

Table 1: Default SPAN Configuration Parameters , on page 16 lists the default settings for SPAN parameters.

Table 1: Default SPAN Configuration Parameters

Parameters	Default
SPAN session	Active. **Note** For Cisco MDS 9700 Series Switches, the default value for Monitor session is Shut.
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 2: Default RSPAN Configuration Parameters , on page 16 lists the default settings for RSPAN parameters.

Table 2: Default RSPAN Configuration Parameters

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

Configuring SPAN

The SPAN feature is specific to switches in the Cisco MDS 9000 Family. It monitors network traffic through a Fibre Channel interface.

Configuring SD Ports for SPAN

Configuring SD Port for SPAN Monitoring

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

Procedure

Step 1 switch# **configure terminal**

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.

Note In Cisco MDS 9700 Series Switches, the switch port speed is 8000 Mbps.

Step 5 switch(config-if)# **no shutdown**

Enables traffic flow through this interface.

Configuring SPAN Session

To configure a SPAN session, follow these steps:

Procedure

Step 1 switch# **configure terminal**

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.

Note In Cisco MDS 9700 Series Switches, SPAN is replaced by Monitor.

Step 3 switch(config)# **no span session 1**

Deletes the specified SPAN session (1).

Step 4 switch(config-span)# **destination interface fc9/1**

Configures the specified destination interface (fc 9/1) in a session.

Step 5 switch(config-span)# **no destination interface fc9/1**

Removes the specified destination interface (fc 9/1).

Step 6 switch(config-span)# **source interface fc7/1**

Configures the source (fc7/1) interface in both directions.

Note While configuring SPAN sources on the Cisco MDS 9124 Fabric Switch, the direction (Rx and Tx) needs to be explicitly mentioned.

Step 7 switch(config-span)# **no source interface fc7/1**

Removes the specified destination interface (fc 7/1) from this session.

Step 8 switch(config-span)# **source interface sup-fc0**

Configures the source interface (sup-fc0) in the session.

Step 9 switch(config-span)# **source interface fc1/5 - 6, fc2/1 -3**

Configures the specified interface ranges in the session.

Step 10 switch(config-span)# **source vsan 1-2**

Configures source VSANs 1 and 2 in the session.

Step 11 switch(config-span)# **source interface port-channel 1**

Configures the source PortChannel (port-channel 1).

Step 12 switch(config-span)# **source interface fcip 51**

Configures the source FCIP interface in the session.

Step 13 switch(config-span)# **source interface iscsi 4/1**

Configures the source iSCSI interface in the session.

Note This is not applicable for MDS 9700 Series Switches.

Step 14 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.

Note This is not applicable for MDS 9700 Series Switches.

Step 15 switch(config-span)# **no source interface port-channel 1**

Deletes the specified source interface (port-channel 1).

Step 16 switch(config-span)# **shutdown**

Temporarily suspends the session.

Note This is applicable for MDS 9700 Series Switches.

Configuring SPAN Filter

To configure a SPAN filter, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **span session 1**

switch(config-span)#

Configures the specified session (1).

Note In Cisco MDS 9700 Series Switches, SPAN is replaced by monitor session 1.

Step 3 switch(config-span)# **source interface fc9/1 tx**

Configures the source fc9/1 interface in the egress (Tx) direction.

Step 4 switch(config-span)# **source filter vsan 1-2**

Configures VSANs 1 and 2 as session filters.

Step 5 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 SPAN sessions in both directions, Rx and Tx.

Note While using Generation 2 fabric switches, you cannot create an additional active SPAN session when you already have one.

You can specify multiple SPAN source interfaces in Rx and Tx directions. However, the direction should be explicitly mentioned at the end of the command. The SPAN will reject any source interface configuration that fails to mention the direction.

Configuring Ingress SPAN Sessions

To configure for ingress SPAN sessions, follow these steps:

Procedure

Step 1 switch# **configure terminal**

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.

Configuring Egress SPAN Session

To configure for egress SPAN sessions, follow these steps:

Procedure

Step 1 switch# **configure terminal**

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.

Examples

This example shows how to configure Cisco MDS 9124 for Multiple SPAN Interfaces

```
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 fc1/2 tx
```

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, which makes 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:

Procedure

Step 1 switch# **configure terminal**

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.

Step 4 switch(config-span)# **no suspend**

Reactivates the session.

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:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **interface fc9/32**

Configures the specified interface.

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.

Step 5 switch(config-if)# **no switchport encap eisl**

Disables (default) the encapsulation option.

Configuring Fibre Channel Analyzers Using SPAN

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

Procedure

Step 1 switch# **configure terminal**

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.

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.

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

Procedure

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.

Configuring Single SD Port to Monitor Traffic

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

Procedure

Step 1 switch# **configure terminal**

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.

Step 4 switch(config-span)# **source interface fc1/1**

Configures the source interface fc1/1 on the same SD port.

Configuring the Source Switch

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

Creating VSAN Interfaces

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

Procedure

Step 1 switchS# **configure terminal**

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

Note
- FC tunnels do not work over nontrunking ISLs.
- The interface cannot be operationally up until the FC tunnel mapping is configured in the destination switch.

To enable the FC tunnel feature, follow these steps:

Procedure

Step 1 switchS# **configure terminal**

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 , follow these steps:

Procedure

Step 1 switchS# **configure terminal**

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.

Configuring the ST Port

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

To configure an ST port, follow these steps:

Procedure

Step 1 switchS# **configure terminal**

Enters configuration mode.

Step 2 switchS(config)# **interface fc2/1**

Configures the specified interface.

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 , follow these steps:

Procedure

Step 1 switchS# **configure terminal**

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.

Configuring 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

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 , follow these steps:

Procedure

Step 1 switchD# **configure terminal**

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).

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 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. This procedure is required to set up the FC tunnel.

Configuring the Destination Switch

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

Configuring VSAN Interfaces

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.

Configuring the SD Port

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

To configure an SD port for the scenario in , follow these steps:

Procedure

Step 1 switchD# **configure terminal**

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

To terminate the FC tunnel in the destination switch for the scenario in , follow these steps:

Procedure

Step 1 switchD# **configure terminal**

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.

Creating Explicit Paths

To create an explicit path for the scenario in , follow these steps:

Before you begin

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.

Procedure

Step 1 switchS# **configure terminal**

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**

Example:

```
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 , 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.

Referencing the Explicit Path

To reference the explicit path, follow these steps:

Procedure

Step 1 switchS# **configure terminal**

Enters configuration mode.

Step 2 switchS(config)# **interface fc-tunnel 100**

References the tunnel ID for Path1.

Step 3 switchS(config)# **explicit-path Path1**

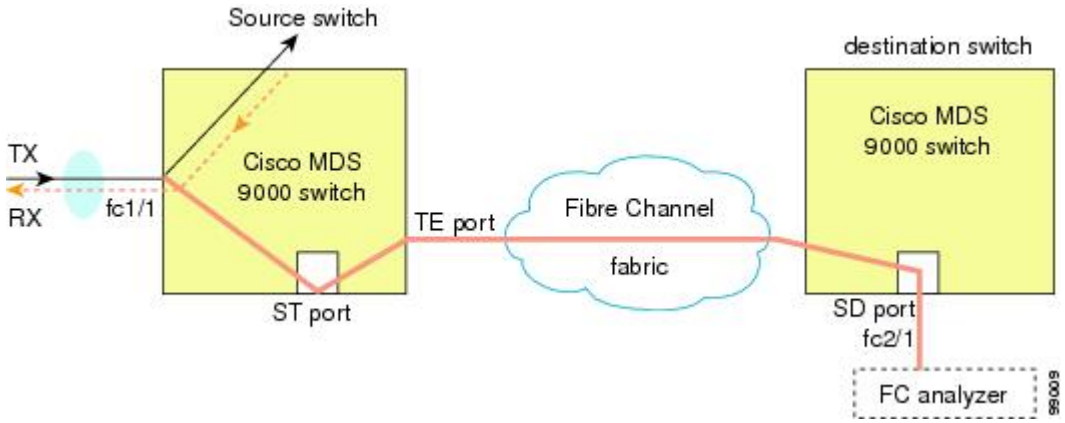
Links Path1 to the tunnel ID.

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 15: Fibre Channel Analyzer Using a Single SD Port to Monitor RSPAN Traffic, on page 30 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 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.

Verifying SPAN Configuration

To display the SPAN configuration information, perform one of the following tasks:

Command	Purpose
show span	Displays SPAN Sessions in a Brief Format **Note** In Cisco MDS 9700 Series Switches, **show span** command is replaced by **show monitor** command.
show span session 7	Displays a Specific SPAN Session in Detail **Note** In Cisco MDS 9700 Series Switches, **show span session 7** command is replaced by **show monitor session 7** command.
show span session	Displays ALL SPAN Sessions **Note** In Cisco MDS 9700 Series Switches, **show span session** command is replaced by **show monitor session all** command.
show int fc9/32	Displays an SD Port Interface with Encapsulation Enabled
show interface brief	Displays ST Port Interface Information
show interface fc1/11	Displays Detailed Information for the ST Port Interface
show fc-tunnel	Displays the FC Tunnel Status
show fc-tunnel tunnel-id-map	Displays FC Tunnel Egress Mapping Information
show fc-tunnel explicit-path	Displays FC Tunnel Explicit Mapping Information
show interface fc-tunnel 200	Displays the FC Tunnel Interface

For detailed information about the fields in the output from these commands, refer to the *Cisco MDS 9000 Family Command Reference* .

Displaying SPAN Information

Use the **show span** command to display configured SPAN information. See the following examples:

SPAN Sessions in a Brief Format

The following example 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
```

Specified SPAN Session in Detail

The following example 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,
```

The following example configures two SPAN sessions to the same destination SD port. This will send bidirectional traffic for the FCIP interface to the destination port.

```
switch# configure
swtch(config)# span session 1
swtch(config-span)# source interface fcip 104 rx
switch(config-span)# destination interface fc1/5

switch# configure
switch(config)# span session 2
switch(config-span)# source interface fcip 104 tx
switch(config-span)# destination interface fc1/5

switch# show span session 1
Session 1 (active)
Destination is fc1/5
   No session filters configured
   Ingress (rx) sources are
     fcip104,
   No egress (tx) sources


switch# show span session 2
Session 2 (active)
Destination is fc1/5
   No session filters configured
   No ingress (rx) sources
   Egress (tx) sources are
     fcip104,
```

ALL SPAN Sessions

The following example 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,
```

SD Port Interface with Encapsulation Enabled

The following example displays 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

Displaying RSPAN Information

Use the **show** commands to display configured RSPAN information. See the following examples:

ST Port Interface Information

The following example 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
```

Detailed Information for the ST Port Interface

The following example 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
```

FC Tunnel Status

The following example displays FC tunnel status:

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

FC Tunnel Egress Mapping Information

The following example 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.

FC Tunnel Explicit Mapping Information

The following example displays FC tunnel 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
```

SPAN Mapping Information

The following example displays the 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,
```

FC Tunnel Interface

The following example 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:
```

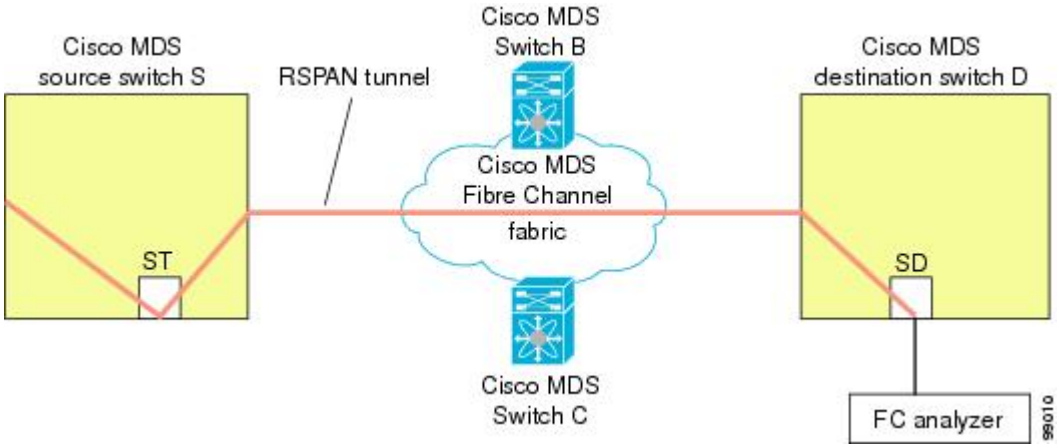
Configuration Examples for RSPAN

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 16: RSPAN Scenario with One Source Switch, One Destination Switch, and One Tunnel, on page 36).

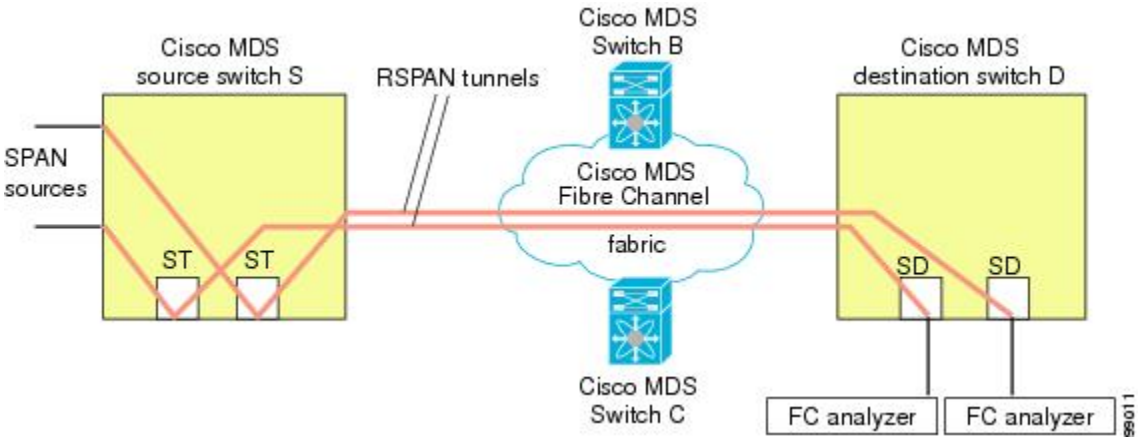
Figure 16: RSPAN Scenario with One Source Switch, One Destination Switch, and One Tunnel



Single Source with Multiple RSPAN Tunnels

Single Source with Multiple RSPAN Tunnels , on page 36 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.

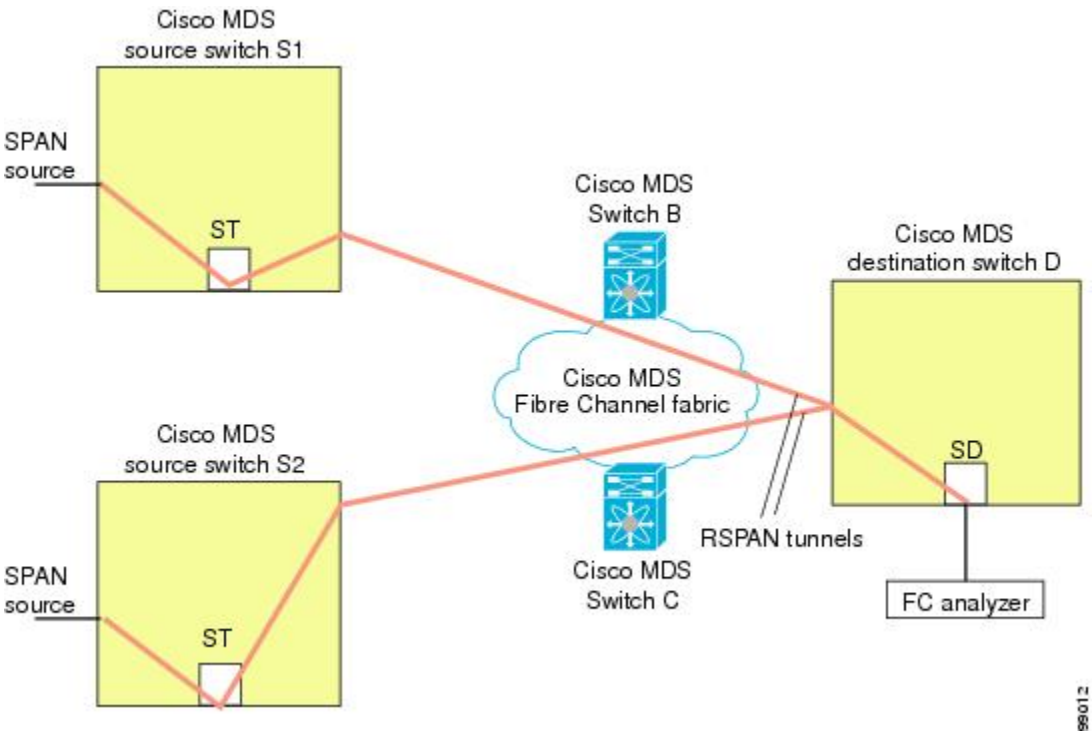
Figure 17: RSPAN Scenario with One Source Switch, One Destination Switch, and Multiple Tunnels



Multiple Sources with Multiple RSPAN Tunnels

Figure 18: RSPAN Scenario with Two Source Switches, a Destination Switch, and Multiple Tunnels, on page 37 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 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.