CHAPTER 30

# 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:

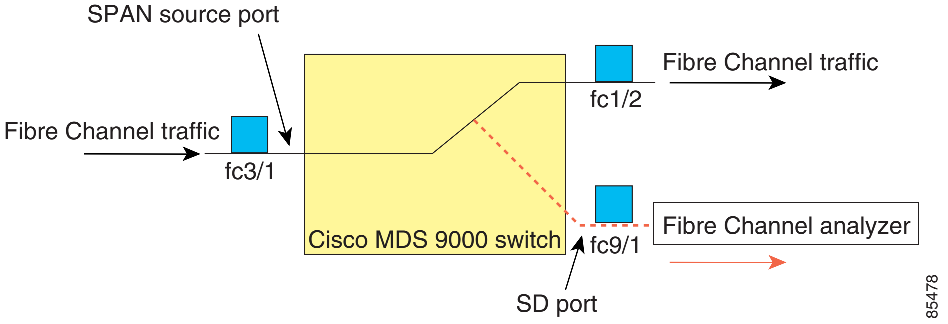
This chapter contains the following topics:

## About SPAN

The switched port analyzer (SPAN) feature is specific to switches in the Cisco MDS 9000 Family. It monitors network traffic though 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 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.

*Figure 30-1* ***SPAN Transmission***

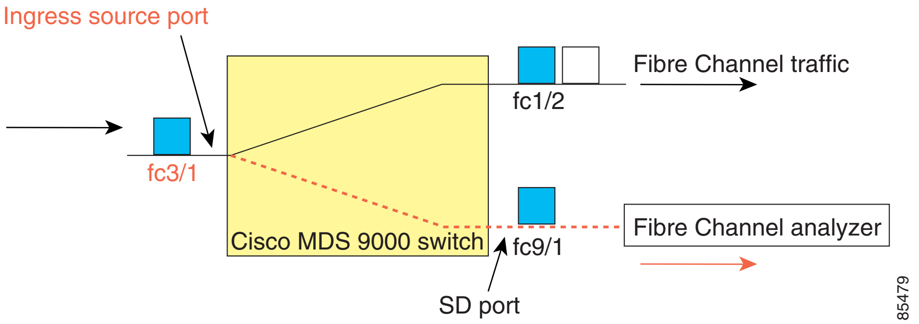


# SPAN Sources

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:

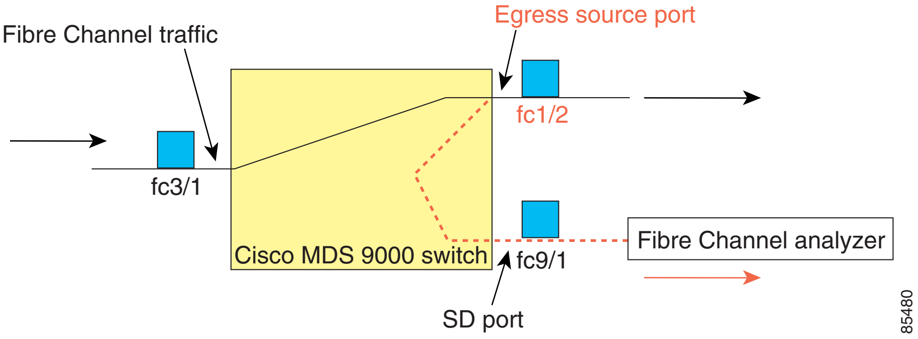
- Ingress source (rx)—Traffic entering the switch fabric through this source interface is spanned or copied to the SD port.

*Figure 30-2* ***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.

*Figure 30-3 SPAN Traffic from Egress Direction*



# IPS Source Ports

Effective SAN-OS Release 1.3(x) Switched Port Analyzer (SPAN) capabilities are also 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 SPAN ingress traffic, egress traffic, or traffic in both directions for all eight iSCSI and 24 FCIP interfaces that are available in the IPS module.

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

## CSM Source Ports

Effective SAN-OS Release 1.3(x) Switched Port Analyzer (SPAN) capabilities are also available on the Caching Services Module (CSM).

Refer to the Cisco MDS 9000 Family SAN Volume Controller Configuration Guide for further information.

# Allowed Source Interface Types

The SPAN feature is available for the following interface types:

- Physical ports
  - 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 interface
- FCIP interfaces

# VSAN as a SPAN 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.

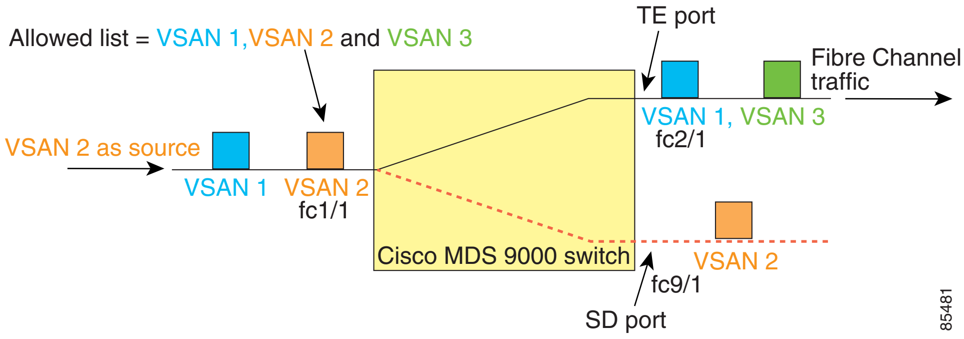
You cannot configure source interfaces (physical interfaces, PortChannels, or sup-fc interfaces) and source VSANs in the same SPAN session.

## 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.
- When a VSAN is specified as a source, you will not be able to 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 SPAN source, you will not be able to 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. displays a configuration using VSAN 2 as a SPAN 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 30-4 VSAN As a SPAN Source***



For the configuration shown in Figure 30-4, the following apply:

- VSAN 2 as a SPAN 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 as the port VSAN does not match VSAN 1.

# 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 a SPAN session, at least one source and the SD port must be up and functioning. Otherwise, traffic will not be directed to the SD port.

To temporarily deactivate (suspend) a SPAN session use the **suspend** command in the SPAN submode. The traffic monitoring is stopped during this time. You can reactivate the SPAN session using the **no suspend** command.

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

# Creating SPAN Sessions

To create a SPAN session, follow these steps.

**Step 1** From the Device Manager, choose **Interface > SPAN**. You see the SPAN dialog box.

**Step 2** Click the **Sessions** tab.

**Step 3** Click **Create**. You see the Create SPAN Session dialog box.

**Step 4** Choose the session ID (from 1-16) using the up or down arrows, and click **Create**.

**Step 5** Repeat Step 4 for each session you want to create.

**Step 6** Click **Close** to close the Create SPAN Session dialog box.

**Step 7** Choose the destination interface by clicking once in the Dest Interface field for the appropriate session.

**Step 8** Choose the filter VSAN list by clicking once in the Filter VSAN List field for the appropriate session.

**Step 9** Choose active or inactive admin status by clicking the Admin drop-down menu and choosing the appropriate status.

**Step 10** Click **Apply** to save your changes, or click **Close** to close the SPAN Sessions dialog box without saving your changes.

# Editing SPAN Sources

To edit a SPAN source, follow these steps.

**Step 1** From the Device Manager, choose **Interface > SPAN**. You see the SPAN dialog box.

**Step 2** Click the **Sources** tab.

**Step 3** Click once on the VSAN List field, and enter the VSAN list name.

**Step 4** Click **Edit FC Source**.

You see the Edit FC Interface Source dialog box.

**Step 5** Click **Create**.

You see the Create FC Interface Source dialog box.

**Step 6** Click the **...** button to display the list of available FC ports. Select a port and click **OK**.

**Step 7** Click the direction (receive or transmit) you want.

**Step 8** Click **Create** to create the FC interface source, or click **Close** to close the Create FC Interface Source dialog box without creating the interface source.

**Step 9** Click **Close**. The new FC interface source is shown in the FC Interface Source dialog box list.

# Deleting SPAN Sessions

To delete a SPAN session, perform the following steps.

**Step 1** From the Device Manager, choose **Interface > SPAN**.

You see the SPAN dialog box.

**Step 2** Click the **Sessions** tab.

**Step 3** Click once to select the SPAN session you want to delete.

**Step 4** Click **Delete**.

The SPAN session is deleted.

# 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. Only VSANs present in the filter are spanned.

You can specify session VSAN filters which 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 buffer-to-buffer 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 port mode can not be changed if it is being used for a SPAN session.

  If you need to change a 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.
- 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 Advanced Services Modules (ASMs).

## Guidelines to Configure SPAN

The following guidelines apply for a SPAN configuration:

- 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.
- 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.

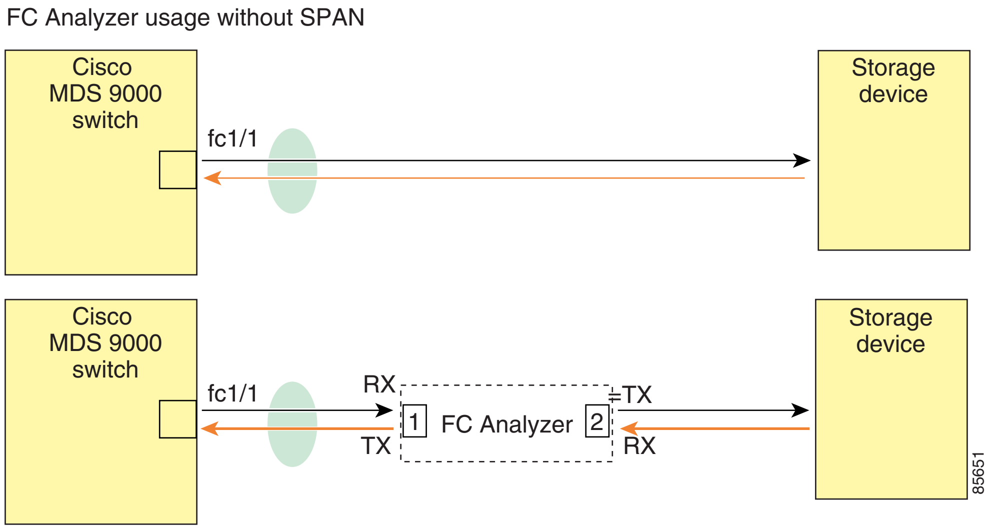
# Monitoring Traffic Using Fibre Channel Analyzers

You can use SPAN to monitor traffic on an interface without any traffic disruption. This feature is specially useful in troubleshooting scenarios when 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 30-5.

*Figure 30-5 Fibre Channel Analyzer Usage Without SPAN*



This type of connection has the following limitations:

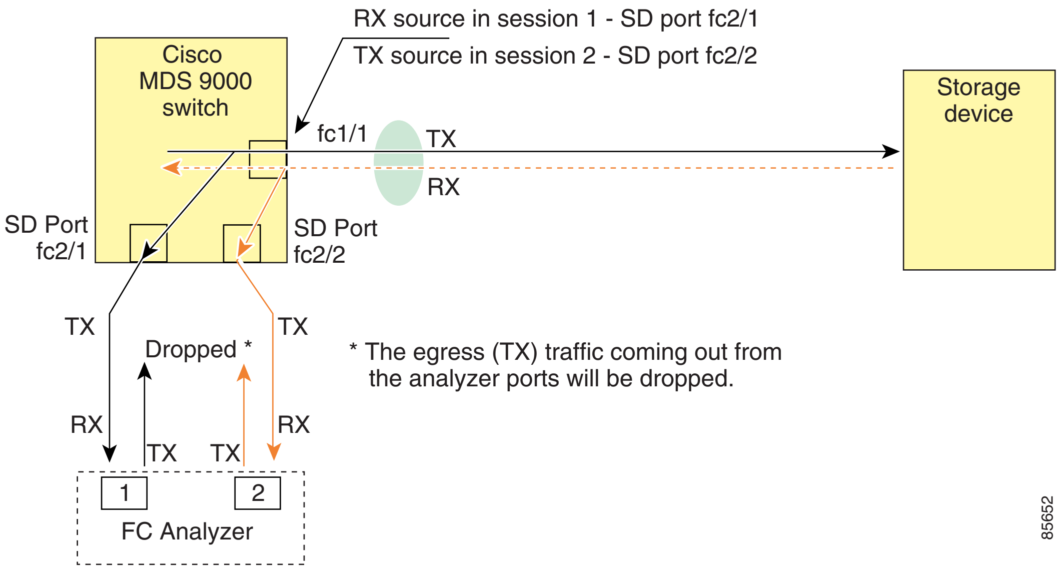
- Requires you to physically insert the FC analyzer between the two network devices.
- It disrupts traffic when the Fibre Channel analyzer is physically connected.
- The analyzer captures data only on the rx links in both port 1 and port 2. Port 1 captures traffic exiting interface fc1/1 and port 2 captures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

# Using SPAN

Using SPAN, you can capture the same traffic scenario shown in Figure 30-5 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 30-6.

*Figure 30-6 Fibre Channel Analyzer Using SPAN*


RX source in session 1 - SD port fc2/1
TX source in session 2 - SD port fc2/2
Cisco MDS 9000 switch
fc1/1
TX
RX
Storage device
SD Port fc2/1
SD Port fc2/2
TX
TX
Dropped *
RX
RX
TX
TX
1
2
FC Analyzer
* The egress (TX) traffic coming out from the analyzer ports will be dropped.
85652

## Configuring Analyzers Using SPAN

To configure Fibre Channel Analyzers using SPAN for the example in Figure 30-6, 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.

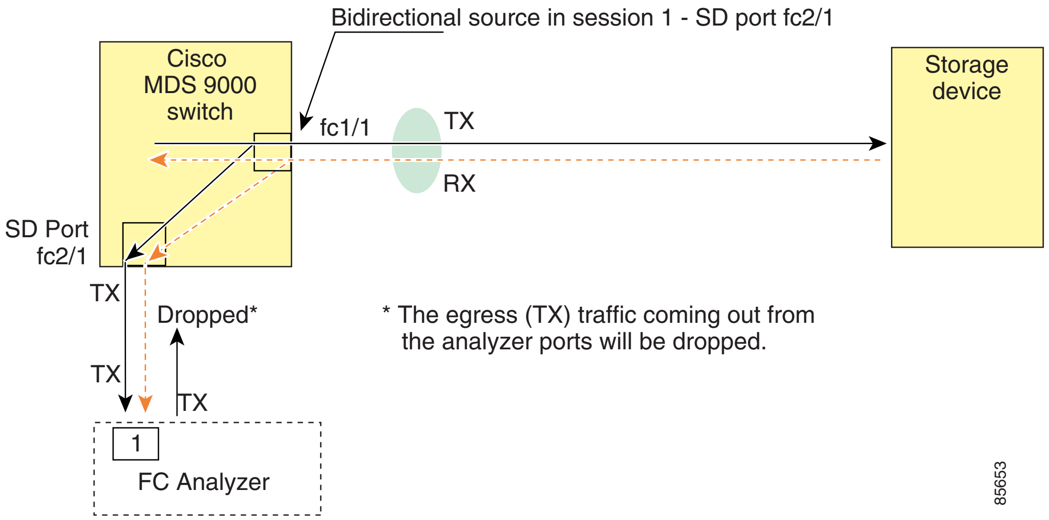
**Step 4** Physically connect fc2/2 to port 2 on the Fibre Channel analyzer.

## Using a 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 30-6. 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 30-7shows 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 direction. This setup is more advantageous and cost-effective than the setup shown in Figure 30-6 because it uses one SD port and one port on the analyzer, instead of using a full, two-port analyzer.

*Figure 30-7 Fibre Channel Analyzer Using a Single SD Port*


Bidirectional source in session 1 - SD port fc2/1
Cisco MDS 9000 switch
fc1/1
TX
RX
Storage device
SD Port fc2/1
TX
Dropped*
TX
TX
1
FC Analyzer
* The egress (TX) traffic coming out from the analyzer ports will be dropped.
85653

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

# Default SPAN Settings

Table 30-1 lists the default settings for SPAN parameters

*Table 30-1 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. |

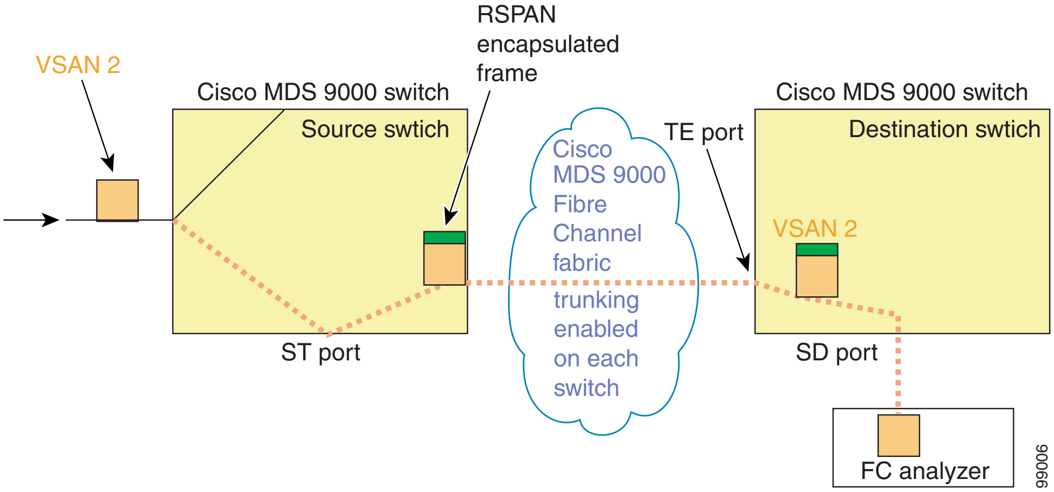
# Remote SPAN

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 MDS source switch.

The RSPAN feature is nonintrusive and does not affect network traffic switching for any 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:

- 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 30-8 RSPAN Transmission***



## Advantages to Using RSPAN

The RSPAN features has the following advantages:

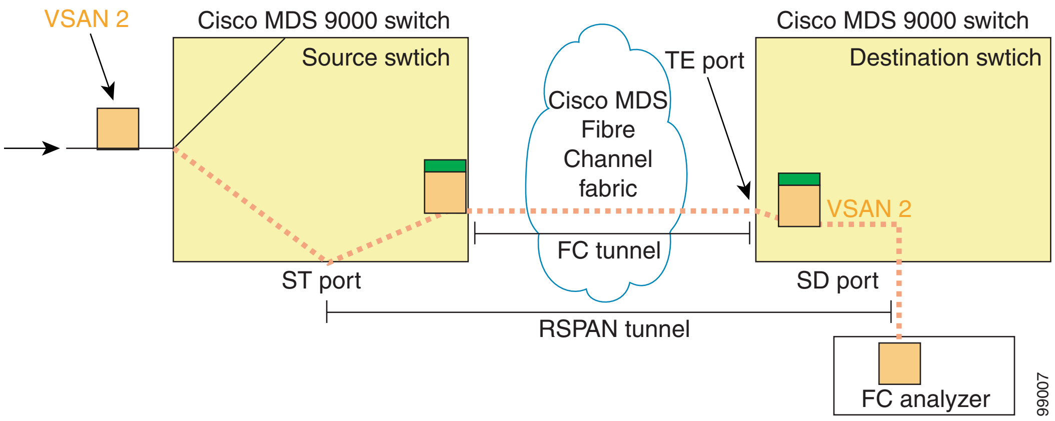
- Enables nondisruptive traffic monitoring at a remote location.
- Provides a cost-effective solution by using one SD port to monitor remote traffic on multiple switches.
- Works with any Fibre Channel analyzer.
- Compatible with the Cisco MDS 9000 Port Analyzer adapters.
- Does not affect traffic in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

## FC and RSPAN Tunnels

A 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 a ST port in the source switch and map the same FC tunnel to a SD port in the destination switch. Once the mapping and binding is configured, the FC tunnel is referred to as a RSPAN tunnel.

*Figure 30-9 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 will be dropped.
- The FC tunnel IP address must reside in the same subnet as the VSAN interface.
- 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 (the **trunk protocol enable** command is enabled by default).
  - VSAN interface must be configured (the **interface vsan** command).
  - The Fibre Channel tunnel feature must be enabled (the **fc-tunnel enable** command is disabled by default).
  - IP routing must be enabled (the **ip routing** command is disabled by default).
- 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.

## ST Port Characteristics

ST port have the following characteristics:

- ST ports perform the RSPAN encapsulation of the FC frame.
- ST ports do not use BB_credits.
- An ST port can only be bound to one FC tunnel.
- ST ports cannot be used for any other purpose other than to carry RSPAN traffic.

- ST Ports cannot be configured using Advanced Services Modules (ASMs).

# 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.

Besides the source and destination switches, the VSAN must also be configured in each 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 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 a RSPAN session in the source switch (in Switch S) to monitor network traffic.

## Configuration in the Source Switch

This section identifies the tasks that must be performed in the source switch (Switch D).

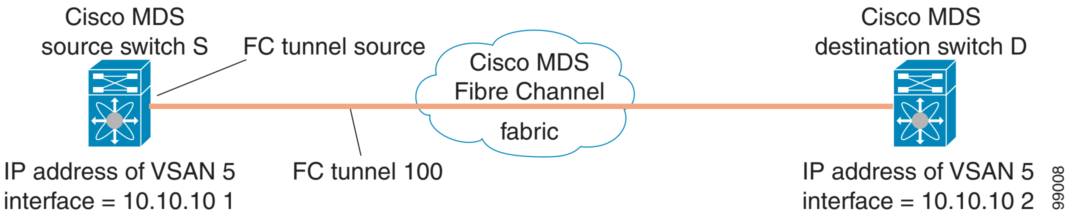
This section contains the following topics:

- Creating VSAN Interfaces, page 30-13
- Configuring the ST Port, page 30-14

### Creating VSAN Interfaces

Figure 30-10 depicts a basic FC tunnel configuration.

*Figure 30-10 FC Tunnel Configuration*

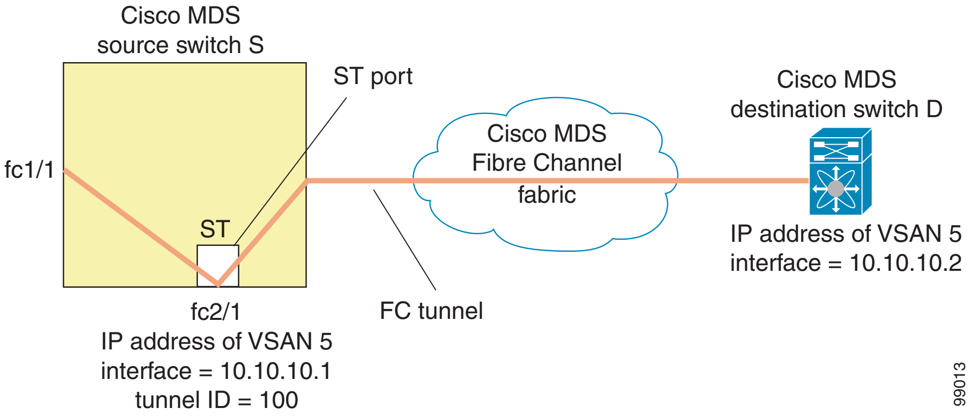


This example assumes that VSAN 5 is already configured in the VSAN database.

### 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 a RSPAN tunnel once the binding and mapping is complete. depicts a basic FC tunnel configuration.

*Figure 30-11 Binding the FC Tunnel*



ST ports cannot be configured using Advanced Services Modules (ASMs).

## 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.

This section contains the following topics:

- Configuring VSAN Interfaces, page 30-14
- Enabling IP Routing, page 30-14

### Configuring VSAN Interfaces

Figure 30-12 depicts an RSPAN tunnel configuration terminating in the destination switch (Switch D).

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

### 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 step is required to setup the FC tunnel.

## Configuration in the Destination Switch

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

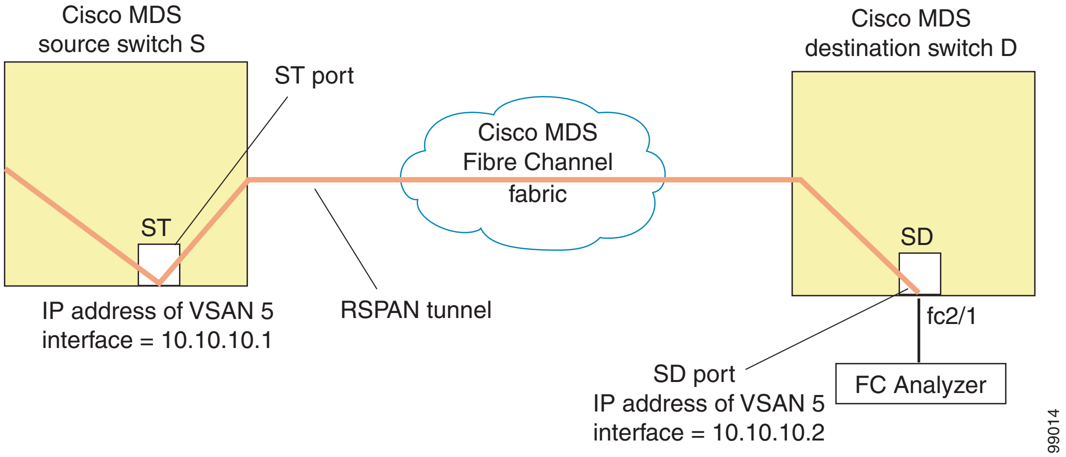
This section contains the following topics:

- Configuring the SD Port, page 30-15
- Mapping the FC Tunnel, page 30-15

### 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. depicts a RSPAN tunnel configuration, now that tunnel destination is also configured.

*Figure 30-12 RSPAN Tunnel Configuration*

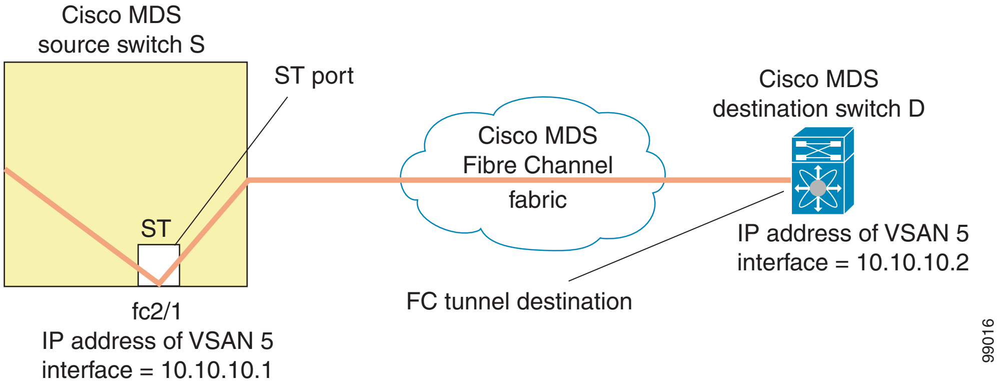


SD ports cannot be configured using Advanced Services Modules (ASMs).

### Mapping the FC Tunnel

The **tunnel-id-map** option specifies the egress interface of the tunnel at the destination switch.

*Figure 30-13 FC Tunnel Configuration*

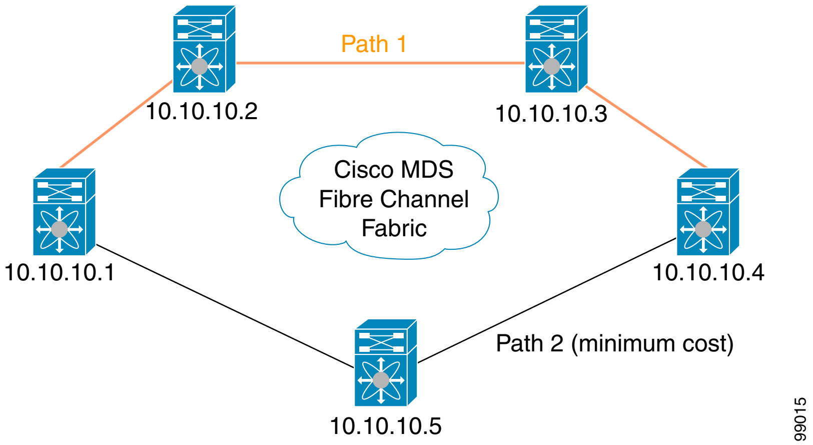


## Configuring An Explicit Path

You can specify an explicit path through the Cisco MDS Fibre channel fabric (source-based routing), use 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 use 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 available. In a 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.

***Figure 30-14 Explicit Path Configuration***



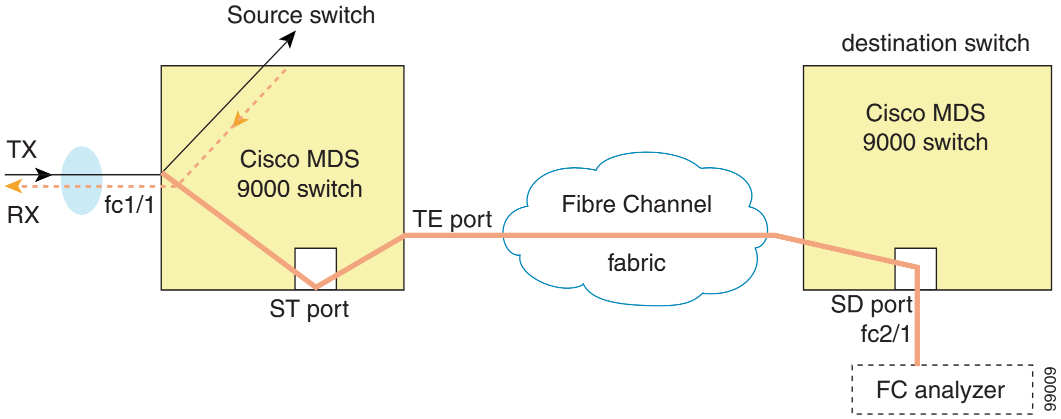
The explicit path must be created in the source switch. To configure an explicit path, you must first create the path and then configure the use of any one path. If an explicit path is not configured, the minimum cost path is used by default. If an explicit path is configured and is functioning, the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

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. shows a 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 direction.

***Figure 30-15 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.

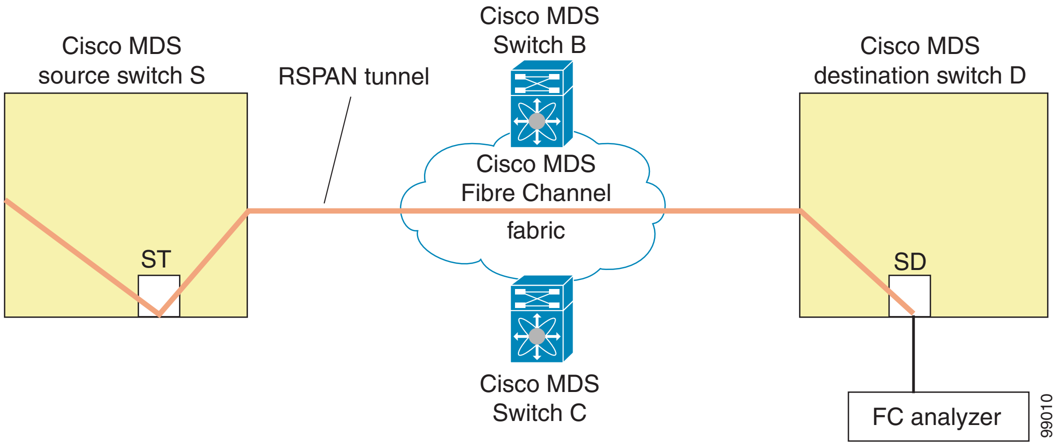
## Sample Scenarios

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. A RSPAN tunnel is configured as a destination interface for SPAN session and the ST port forwards SPAN traffic through the RSPAN tunnel.

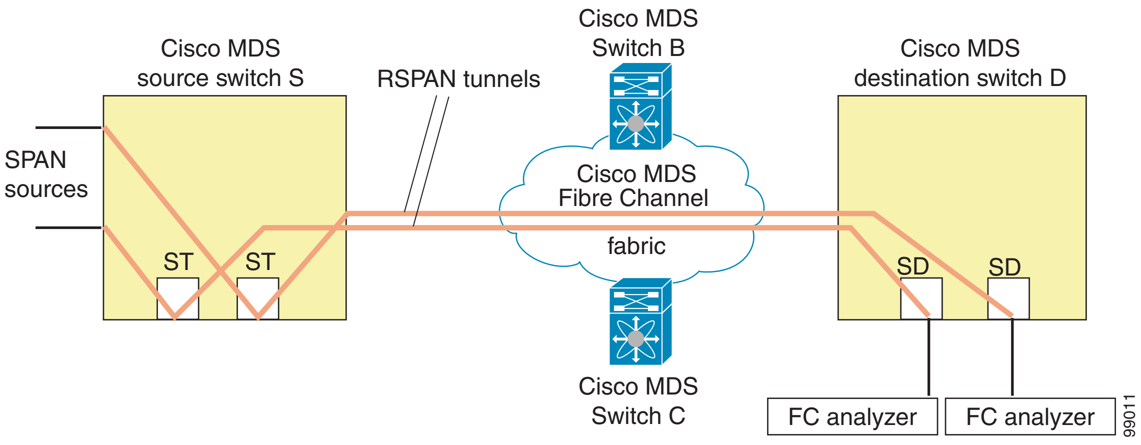
*Figure 30-16 RSPAN Scenario with One Source Switch, One Destination Switch, and One Tunnel*



### Single Source with Multiple RSPAN Tunnels

Figure 30-17 displays two separate RSPAN tunnels configured between Switches S and D. 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 trouble shooting purposes.

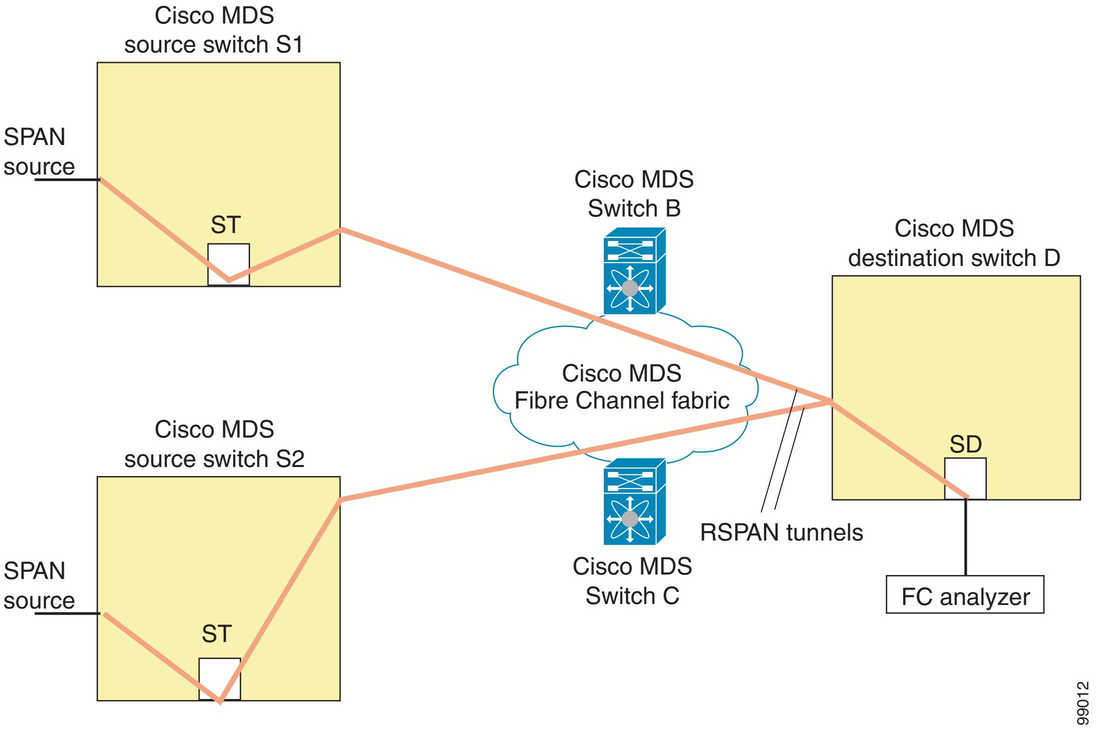
*Figure 30-17* ***RSPAN Scenario with One Source Switch, One Destination Switch, and Multiple Tunnels***



## Multiple Sources with Multiple RSPAN Tunnels

Figure 30-18 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 30-18* ***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.