



CHAPTER 10

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, page 10-2](#)
- [SPAN Sources, page 10-2](#)
- [SPAN Sessions, page 10-5](#)
- [Specifying Filters, page 10-5](#)
- [SD Port Characteristics, page 10-5](#)
- [Configuring SPAN, page 10-6](#)
- [Monitoring Traffic Using Fibre Channel Analyzers, page 10-10](#)
- [Default SPAN Settings, page 10-13](#)

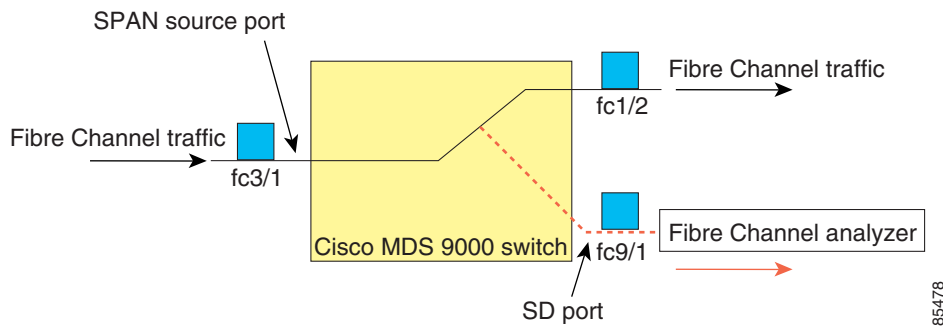
[Send documentation comments to fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)

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 non-intrusive and does not affect switching of network traffic for any SPAN source ports (see Figure 10-1).

Figure 10-1 SPAN Transmission



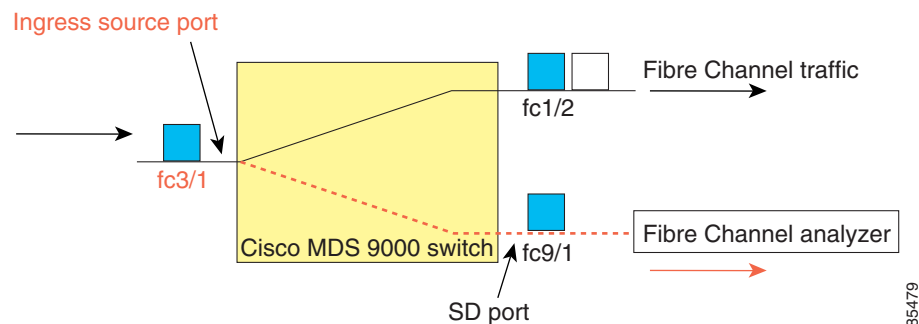
85478

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 10-2).

Figure 10-2 SPAN Traffic from the Ingress Direction

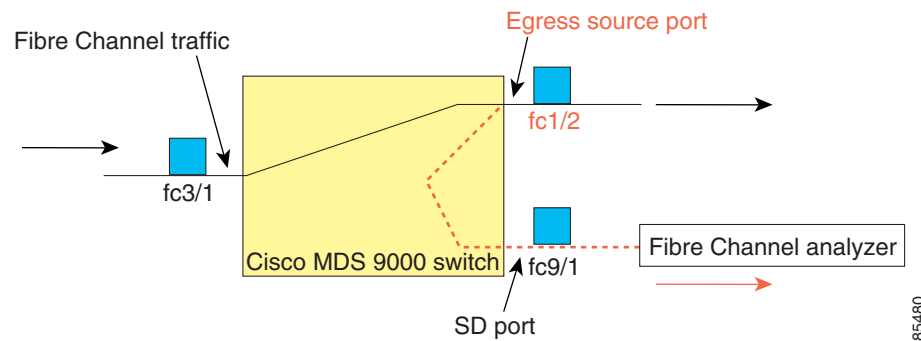


85479

- Egress source (Tx)—Traffic exiting the switch fabric through this source interface is *spanned* or copied to the SD port (see Figure 10-3).

Send documentation comments to fm-docfeedback@cisco.com

Figure 10-3 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

Send documentation comments to fm-docfeedback@cisco.com

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.

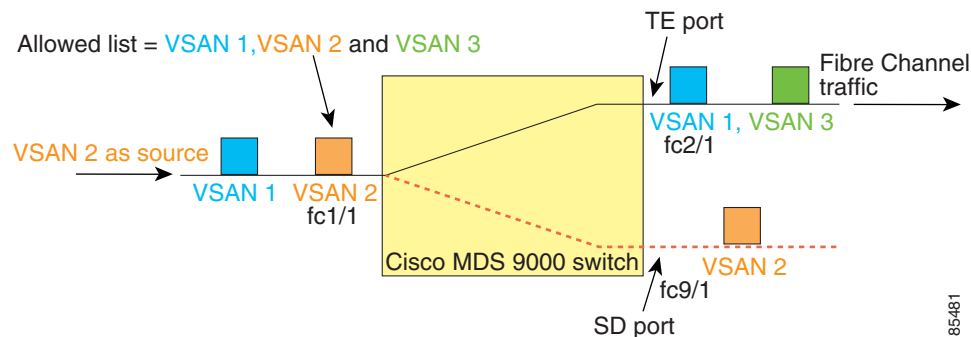
You cannot configure source interfaces (physical interfaces, PortChannels, or sup-fc interfaces) and source VSANs in the same SPAN session.

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 10-4](#) 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 10-4 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.

85481

Send documentation comments to fm-docfeedback@cisco.com

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 10-4](#)). 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.

Send documentation comments to fm-docfeedback@cisco.com

- 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.

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.
- 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.
-

Configuring SPAN

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

-
- Step 1** Right-click the port you want to configure and select **Configure**.
You see the general port configuration dialog.
 - Step 2** Under Mode, choose **SD**.
 - Step 3** Click **Apply** to accept the change.
 - Step 4** Close the dialog box.
-

Send documentation comments to fm-docfeedback@cisco.com

Configuring SPAN max-queued-packets

When a SPAN destination port is oversubscribed or has more source traffic than the speed of the destination port, the source ports of the SPAN session will reduce in their throughput. The impact is proportional to the amount of source traffic flowing in. Lowering the max-queued-packets value from the default value of 15 to 1 prevents the impact on the source ports. It is necessary to reconsider the default value for this setting as it may impact the source interface throughput.

By default, SPAN frames are dropped if the sum of the bandwidth of the source interfaces exceed the bandwidth of the destination port. With a higher value, the SPAN traffic has a higher probability of reaching the SPAN destination port instead of being dropped at the expense of data traffic throughput.



Note

The span max-queued-packets can be changed only if no span sessions are currently active on the switch.



Note

If you are spanning the traffic going through an FCIP interface, span copies may be dropped even if the SD interface has more bandwidth than the amount of traffic being replicated. To avoid span drops, set the max-queued-packets to a higher value; for example, 100.

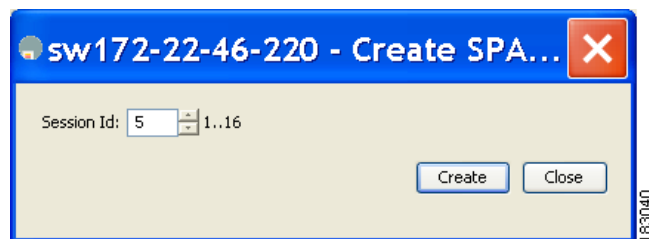
Creating SPAN Sessions

To create SPAN sessions using Device Manager, follow these steps:

- Step 1** Choose **Interface > SPAN**. You see the SPAN dialog box.
- Step 2** Click the **Sessions** tab.
- Step 3** Click **Create**.

You see the Create SPAN Sessions dialog box shown in [Figure 10-5](#).

Figure 10-5 Create SPAN Sessions 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** Enter the destination interface in the Dest Interface field for the appropriate session.
- Step 7** Enter the filter VSAN list in the Filter VSAN List field for the appropriate session.
- Step 8** Choose **active** or in **active** admin status in the Admin drop-down list.
- Step 9** Click **Apply** to save your changes.

Send documentation comments to fm-docfeedback@cisco.com

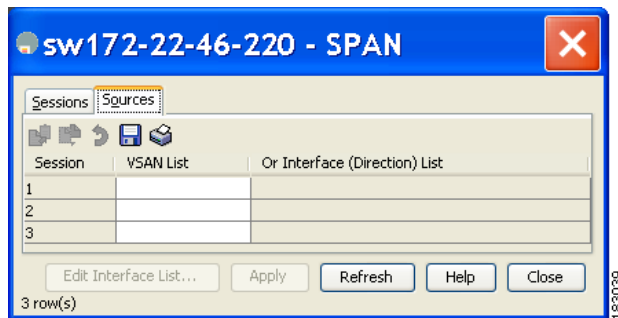
Step 10 Close the two dialog boxes.

Editing SPAN Sources

To edit a SPAN source using Device Manager, follow these steps:

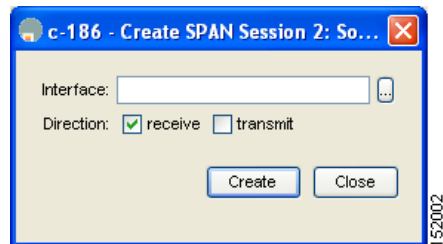
- Step 1** Choose **Interface > SPAN**.
You see the SPAN dialog box.
- Step 2** Click the **Sources** tab.
You see the dialog box shown in [Figure 10-6](#).

Figure 10-6 SPAN Sources Tab



- Step 3** Enter the VSAN list name in the VSAN List field.
- Step 4** Click **Edit Interface List**.
You see the Source Interfaces dialog box.
- Step 5** Click **Create**.
You see the Source Interfaces Interface Sources dialog box shown in [Figure 10-7](#).

Figure 10-7 Source Interfaces Interface Sources Dialog Box



- Step 6** Click the browse button to display the list of available FC ports.
- Step 7** Choose a port and click **OK**.
- Step 8** Click the direction (**receive** or **transmit**) you want.
- Step 9** Click **Create** to create the FC interface source.

Send documentation comments to fm-docfeedback@cisco.com

Step 10 Click **Close** in each of the three open dialog boxes.

Deleting SPAN Sessions

To delete a SPAN session using Device Manager, follow these steps:

-
- Step 1** Choose **Interface > SPAN**.
You see the SPAN dialog box.
- Step 2** Click the **Sessions** tab.
- Step 3** Click the SPAN session you want to delete.
- Step 4** Click **Delete**.
The SPAN session is deleted.
- Step 5** Close the dialog box.
-

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):

Send documentation comments to fm-docfeedback@cisco.com

```
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

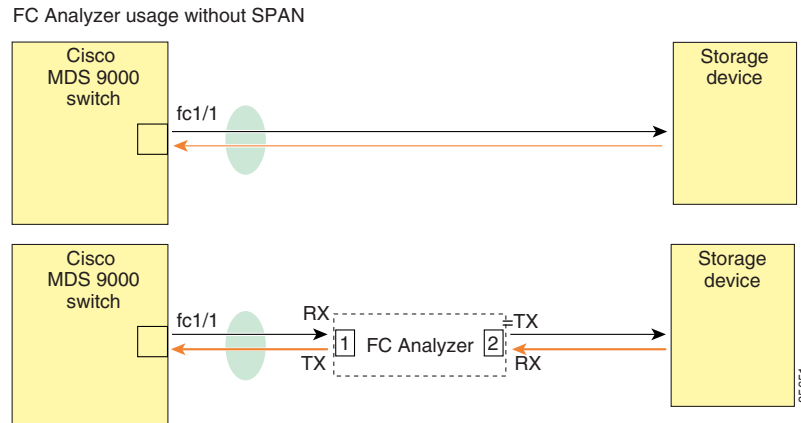
You can use SPAN to monitor traffic on an interface without any traffic disruption. This feature is especially useful in troubleshooting scenarios where traffic disruption changes the problem environment and makes it difficult to reproduce the problem.

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 10-8](#).

Send documentation comments to fm-docfeedback@cisco.com

Figure 10-8 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.

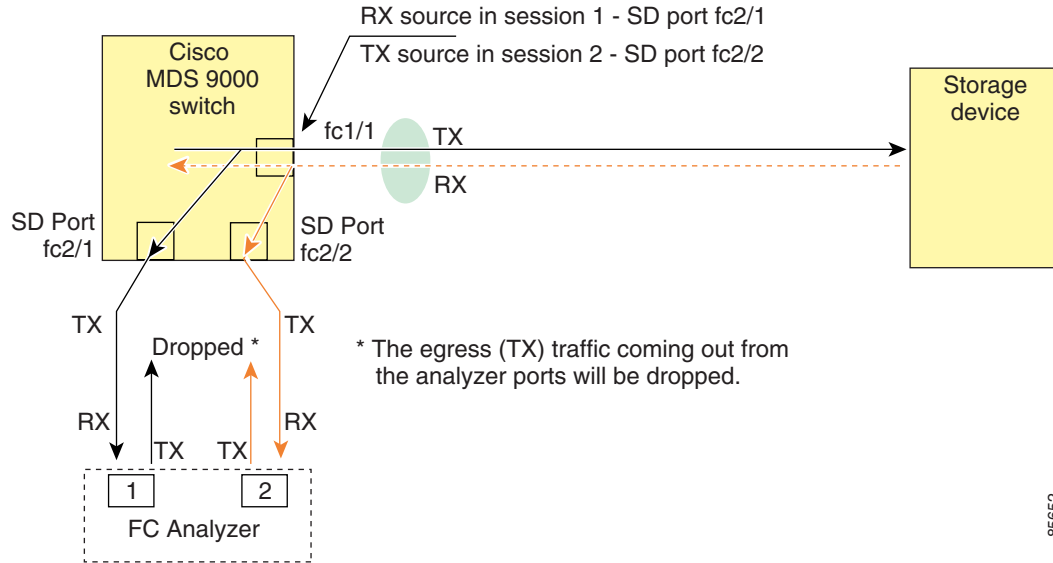
With SPAN

Using SPAN you can capture the same traffic scenario shown in [Figure 10-8](#) 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 10-9](#).

Send documentation comments to fm-docfeedback@cisco.com

Figure 10-9 Fibre Channel Analyzer Using SPAN



Configuring Fibre Channel Analyzers Using SPAN

To configure Fibre Channel Analyzers using SPAN for the example in [Figure 10-9](#), 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 fc1/1 in 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.

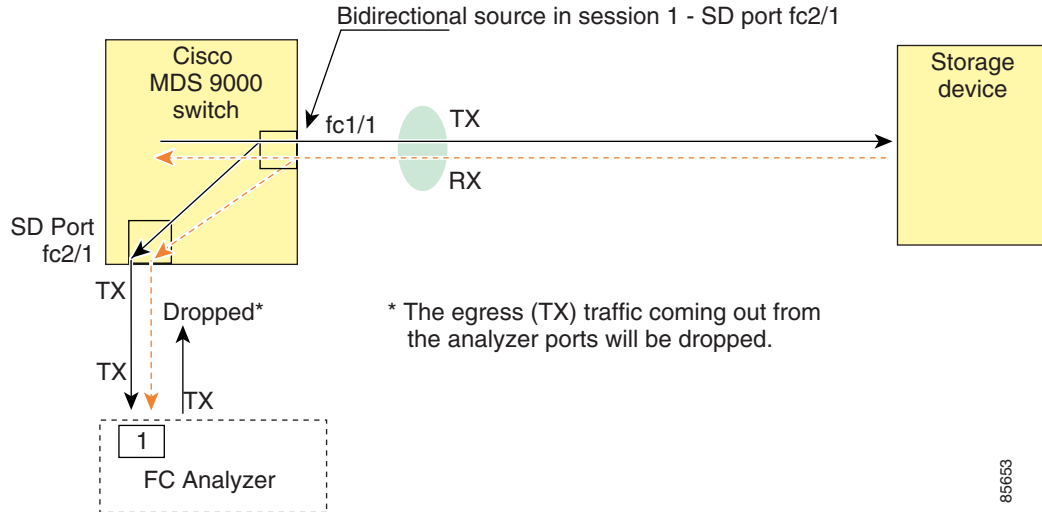
Single SD Port to Monitor Traffic

You do not need to use two SD ports to monitor bidirectional traffic on any interface as shown in [Figure 10-9](#). 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 10-10](#) 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 10-9](#)—it uses one SD port and one port on the analyzer, instead of using a full, two-port analyzer.

Send documentation comments to fm-docfeedback@cisco.com

Figure 10-10 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.

Default SPAN Settings

Table 10-1 lists the default settings for SPAN parameters.

Table 10-1 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.

Send documentation comments to fm-docfeedback@cisco.com