Monitoring Network Traffic Using SPAN

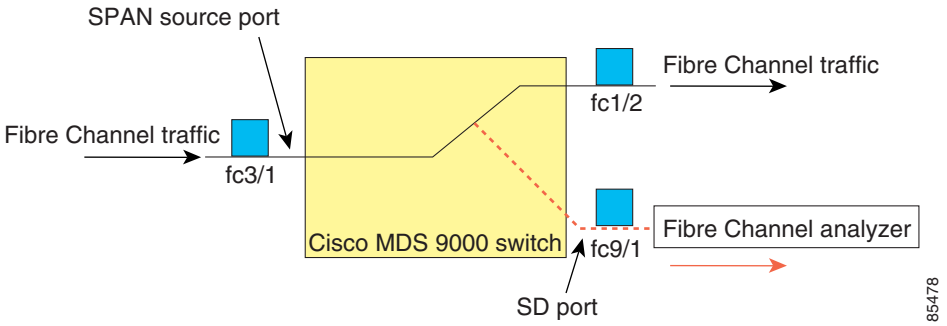
This chapter describes the switched port analyzer (SPAN) features provided in switches in the Cisco MDS 9000 Family. It includes the following sections:

About SPAN

The 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 (see "Configuring a Fabric Analyzer" section on page 23-5).

SD ports do not receive frames, they merely transmit a copy of the SPAN source traffic. The SPAN feature is non-intrusive and does not affect switching of network traffic for any SPAN source ports (see Figure 22-1).

Figure 22-1 SPAN Transmission

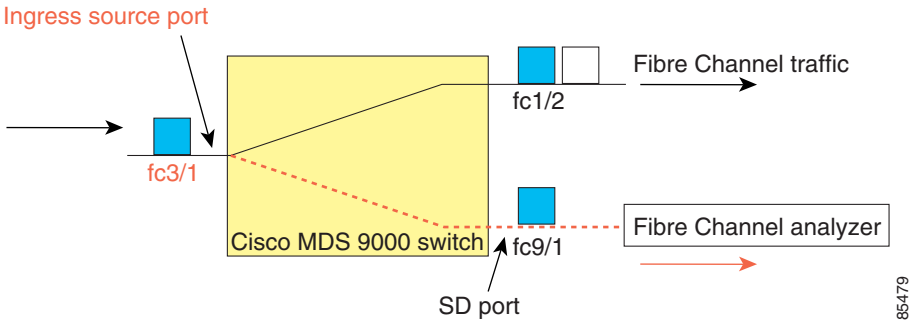


SPAN Sources

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

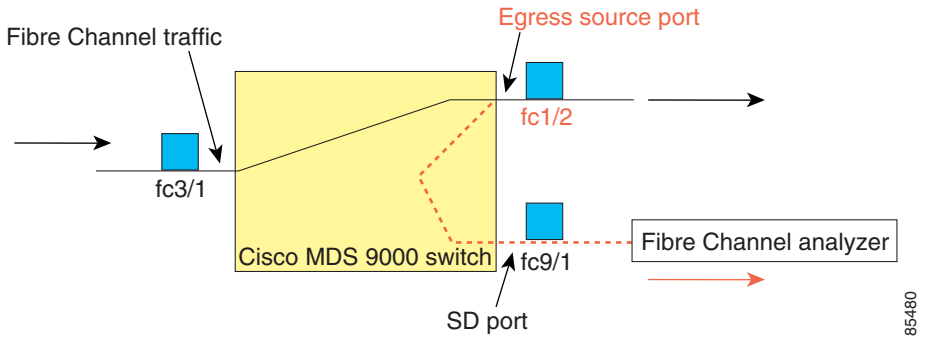
- Ingress source (rx)—Traffic entering the switch fabric through this source interface is *spanned* or copied to the SD port (see Figure 22-2).

Figure 22-2 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 22-3).

Figure 22-3 SPAN Traffic from Egress Direction



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.

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.

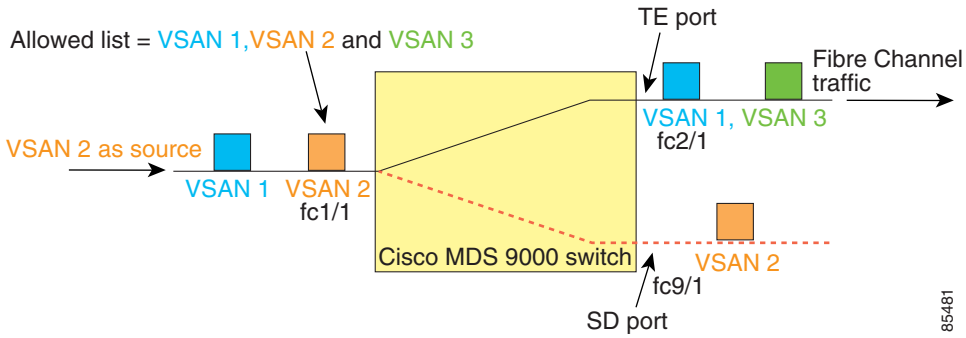
Guidelines to Configure VSANs as a Source

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 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. Figure 22-4 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 22-4 VSAN As a SPAN Source



For this configuration, 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. See "Configuring Trunk-Allowed VSAN List" section on page 10-4 or "VSAN Membership" section on page 8-5.

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.

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

Specifying Filters

You can perform VSAN-based filtering to selectively monitor network traffic on specified VSANs. You can apply this VSAN filter to the selected source or to all sources in a session (see Figure 22-4). Only traffic in the selected VSANs is spanned when you configure VSAN filters.

You can specify two types of VSAN filters:

- Interface level filters—You can apply VSAN filters for a specified TE port or trunking PortChannel to filter traffic using one of three options: the ingress direction, the egress direction, or both directions.
- Session filters—filters 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:

- Specify filters in either the ingress direction, or in the egress direction, or in both directions.
- PortChannel filters are applied to all ports in the PortChannel.
- If no filters are specified, the traffic from all active VSANs for that interface is spanned.
- The effective filter on a port is the intersection (filters common to both) of interface filters and session filters.
- While you can specify any arbitrary VSAN filters in an interface, traffic can only be monitored on the port VSAN or on allowed-active VSANs in that interface.
- When you configure VSAN as a source, that VSAN is implicitly applied as an interface filter to all sources included in the specified VSAN.

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.

Note 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.

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 (see the "Configuring 32-port Switching Modules" section on page 9-7).
- SPAN frames are dropped if the sum of the bandwith 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 SPAN session.

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

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

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# interface fc9/1`	Configures the specified interface.
Step 3	`switch(config-if)# switchport mode SD`	Configures the SD port-mode for interface fc2/1.
Step 4	`switch(config-if)# switchport speed 1000`	Configures the SD port speed to 1000 Mbps.
Step 5	`switch(config-if)# no shutdown`	Enables traffic flow.

To configure a SPAN session, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# span session 1` `switch(config-span)#`	Configures the specified SPAN session (1). If the session does not exist, it will be created.
	`switch(config)# no span session 1`	Deletes the specified SPAN session (1).
Step 3	`switch(config-span)# destination interface fc9/1`	Configures the specified destination interface (fc 9/1) in a session.
	`switch(config-span)# no destination interface fc9/1`	Removes the specified destination interface (fc 9/1).

	Command	Purpose
Step 4	`switch(config-span)# source interface fc7/1`	Configures the source (fc7/1) interface in both directions.
	`switch(config-span)# no source interface fc7/1`	Removes the specified destination interface (fc 7/1).
Step 5	`switch(config-span)# source interface sup-fc0`	Configures the source interface (sup-fc0) in the session.
	`switch(config-span)# source interface fc1/5 - 6, fc2/1 -3`	Configures the specified interface ranges in the session.
	`switch(config-span)# source vsan 1-2`	Configures the source VSAN 1 in the session.
	`switch(config-span)# source interface port-channel 1`	Configures the source PortChannel (port-channel 1).
	`switch(config-span)# no source interface port-channel 1`	Deletes the specified source interface (port-channel 1)
Step 6	`switch(config-span)# suspend`	Suspends the session.
	`switch(config-span)# no suspend`	Reactivates the session.

To configure a SPAN filter, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# span session 1` `switch(config-span)#`	Configures the specified session (1).
Step 3	`switch(config-span)# source interface fc9/1 tx filter vsan 1`	Configures VSAN 1 as a filter on the source fc9/1 interface in the egress (tx) direction
	`switch(config-span)# source filter vsan 1-2`	Configures these VSANs as session filters.
	`switch(config-span)# source interface fc7/1 rx`	Configures the VSAN filter on source fc7/1 interface in the ingress (rx) direction.

Encapsulating Frames

The **switchport encap eisl** command only applies to SD port interfaces. This command is disabled by default. If you enable the encapsulation feature, all outgoing frames will be encapsulated. If encapsulation is enabled, you will see a new line (`Encapsulation is eisl`) in the **show int** *SD_port_interface* command output.

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

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# interface fc9/32`	Configures the specified interface.
Step 3	`switch(config-if)# switchport mode SD`	Configures the SD port-mode for interface fc2/1.
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 the encapsulation option and reverts the switch to factory default.

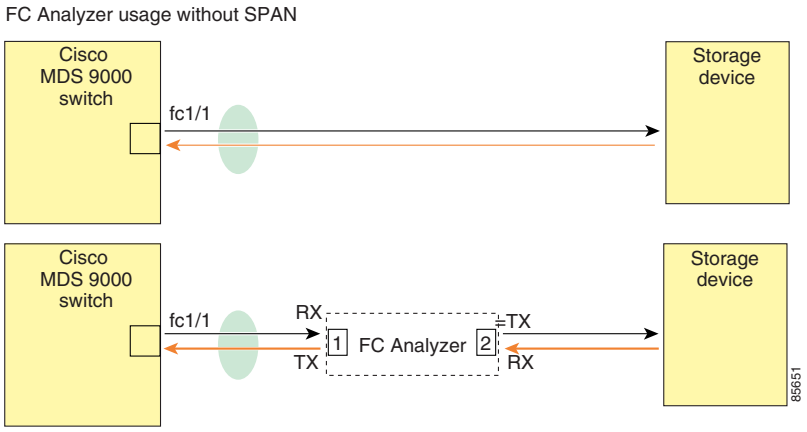
Monitoring Traffic Using Fibre Channel Analyzers

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 22-5.

Figure 22-5 Fibre Channel Analyzer Usage Without SPAN



This type of connection has the following limitations:

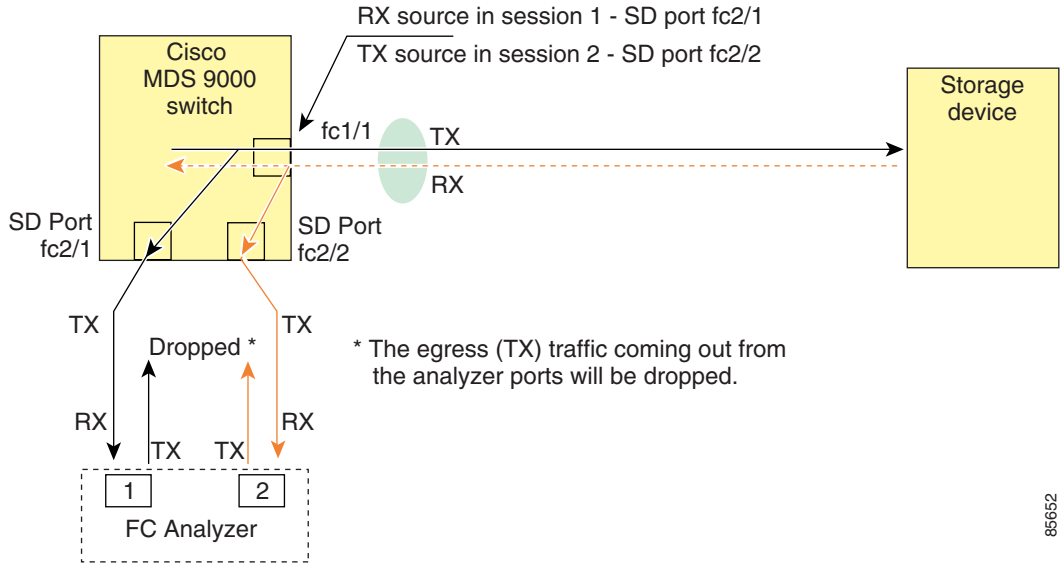
- Requires you to physically insert the FC analyzer between the two network devices.
- It disrupts traffic when the Fibre Channel analyzer is physically connected.
- The analyzer captures data only on the rx links in both port 1 and port 2. Port 1 captures traffic exiting interface fc1/1 and port 2 captures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

Using SPAN

Using SPAN you can capture the same traffic scenario shown in Figure 22-5 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 fc2/1 and egress traffic on SD port fc2/2. This traffic is seamlessly captured by the FC analyzer as shown in Figure 22-6.

Figure 22-6 Fibre Channel Analyzer Using SPAN



Configuring Analyzers Using SPAN.

To configure Fibre Channel Analyzers using SPAN for the example in Figure 22-6, follow these steps:

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

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

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

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

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

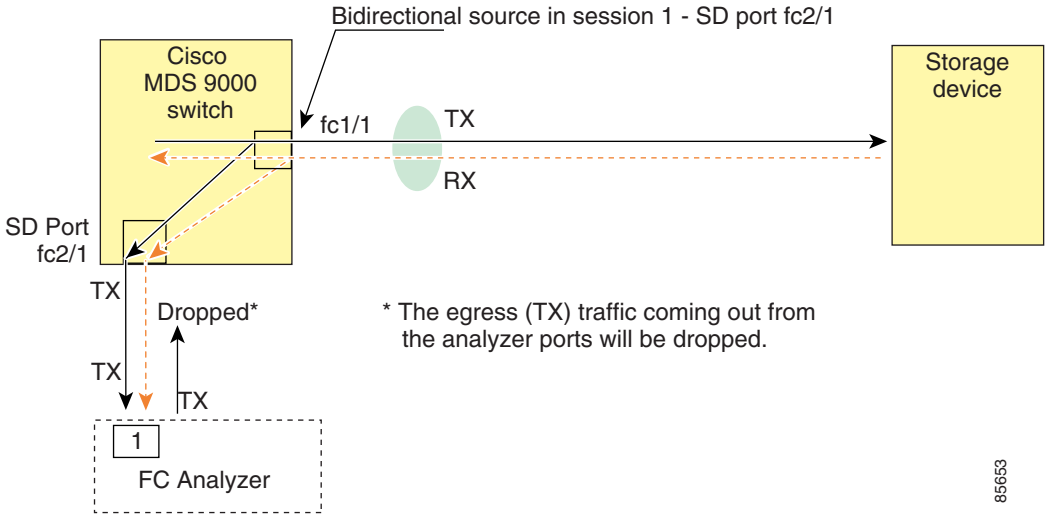
	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# span session 1` `switch(config-span)#`	Creates the SPAN session 1.
Step 3	`switch(config-span)## destination interface fc2/1`	Configures the destination interface fc2/1.
Step 4	`switch(config-span)# source interface 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.

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 22-6. 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 22-7 shows a SPAN setup where one session with destination port fc2/1 and source interface fc1/1 is used to capture traffic in both ingress and egress direction. This setup is more advantageous and cost-effective than the setup shown in Figure 22-6—it uses one SD port and one port on the analyzer, instead of using a full, two-port analyzer.

Figure 22-7 Fibre Channel Analyzer Using a Single SD Port



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

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

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# span session 1` `switch(config-span)#`	Creates the SPAN session 1.
Step 3	`switch(config-span)## destination interface fc1/1`	Configures the destination interface fc1/1.
Step 4	`switch(config-span)# source interface fc1/1`	Configures the source interface fc1/1 on the same SD port.

Displaying SPAN Information

Use the **show span** command to display configured SPAN information. See Examples 22-1 to 22-4.

Example 22-1 Displays SPAN Sessions in a Brief Format

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

Example 22-2 Displays a Specific SPAN Session Details

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

Example 22-3 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
     sup-fc0,
   Egress (tx) sources are
     sup-fc0,
Session 3 (admin suspended)
   Destination is not configured
   Session filter vsans are 1-20
   Ingress (rx) sources are
     fc3/2 (vsan 1-2), fc3/3 (vsan 1-2), fc3/4 (vsan 1-2),
     port-channel 2 (vsan 1-10),
   Egress (tx) sources are
     fc3/2 (vsan 1-2), fc3/3 (vsan 1-2), fc3/4 (vsan 1-2),
```

Example 22-4 Displays an SD-port Interface with Encapsulation Enabled

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

Default Settings

Table 22-1 lists the default settings for SPAN parameters

Table 22-1 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.