Cisco MDS 9000 Family Port Analyzer Adapter Installation and Configuration Note

Text Part Number: OL-9077-01

This document describes the Cisco MDS 9000 Family Port Analyzer Adapter (DS-PAA and DS-PAA2), and the procedures required to install and configure it. It also describes setting up Cisco Traffic Analyzer and Cisco Protocol Analyzer solutions. This installation and configuration note includes the following sections:

Overview

The PAA enables effective, low-cost analysis of Fibre Channel traffic. The device is a standalone Fibre Channel-to-Ethernet adapter, designed primarily to analyze Fibre Channel Switched Port Analyzer (SPAN) traffic from a Fibre Channel port on a Cisco MDS 9000 Family switch. The main function of the adapter is to encapsulate Fibre Channel frames into Ethernet frames. This encapsulation allows low-cost analysis of Fibre Channel traffic while leveraging the existing Ethernet infrastructure.

The PAA allows you to examine Fibre Channel frames of various sizes. Fibre Channel frames from Layers 2, 3, and 4 may be examined without network disruption.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

The PAA works in conjunction with the SPAN feature on the Cisco MDS 9000 Family of switches. The SPAN feature allows storage network administrators to nondisruptively replicate any port's traffic to any other port that is programmed as a SPAN destination(SD port). It encapsulates the Fibre Channel frames from the SD port into Ethernet frames that can be analyzed on a PC. Storage administrators can troubleshoot the network quickly and cost-effectively, with no network disruption.

You can copy frames using the Cisco Protocol Analyzer or the Cisco Traffic Analyzer. The Cisco Protocol Analyzer is a modified version of Ethereal, and the Cisco Traffic Analyzer is a modified version of nTop, a network traffic probe. Both analyzers are modified to support Fibre Channel and SCSI.

Note Additional information about Ethereal is available at http://www.ethereal.com, and additional information about the Cisco Traffic Analyzer is available at http://www.cisco.com/kobayashi/sw-center/sw-stornet.shtml.

The PAA sets appropriate bits in the encapsulated trailer to indicate different types of errors (for example, CRC-errors, empty frame, jumbo frame, or other errors) during a data transfer. Both the Cisco Protocol Analyzer and the Cisco Traffic Analyzer can decode these packets, but they do so for different purposes. The Cisco Traffic Analyzer decodes packets for traffic analysis, and the Cisco Protocol Analyzer decodes packets for protocol analysis.

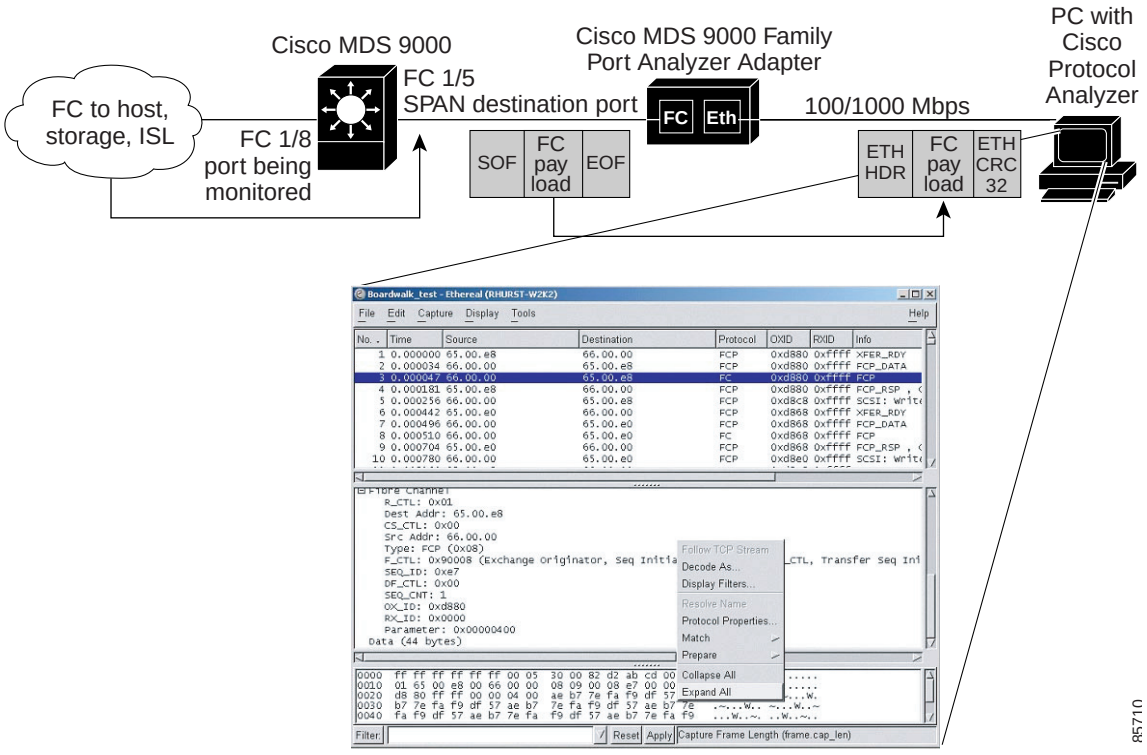
The adapter has two primary interfaces:

- A Fibre Channel interface that operates at 1-Gbps or 2-Gbps
- A 100/1000-Mbps Ethernet port

Note The 1-Gbps and 2-Gbps Fibre Channel links do not support auto negotiation. You must explicitly configure the link speed.

Figure 1 shows the PAA connected to a Fibre Channel port acting as an SD port on the Cisco MDS 9000 Family switch. The switch is connected by Ethernet to the PC that is running Cisco Protocol Analyzer.

Figure 1 Cisco MDS 9000 Family Port Analyzer Adapter Network Topology Example



Installation Requirements

Before using the adapter in a network, verify the following:

- The Fibre Channel port on the Cisco MDS 9000 Family switch must be configured as an SD port, as described in the *Cisco MDS 9000 Family CLI Configuration Guide* or the *Cisco MDS 9000 Family Fabric Manager Guide*. For more information, see the "Cisco MDS 9000 SPAN Usage Instructions" section on page 4.
- Cisco Traffic Analyzer or Cisco Protocol Analyzer must be installed on the PC attached to the adapter, as described in the "Setting Up the Cisco Traffic Analyzer" section on page 15 and the "Setting Up the Cisco Protocol Analyzer" section on page 22.
- The adapter must be used in one of four truncate modes, which can be set using the four Dual Inline Package (DIP) switches on the rear of the unit. See the "Modes of Operation" section on page 7 for the correct mode.
- The Fibre Channel interface on the adapter must then be connected to the Fibre Channel SD port on the Cisco MDS 9000 Family switch.
- The Ethernet interface adapter must be connectedeither to the host that is using Cisco Traffic Analyzer or Cisco Protocol Analyzer software, or to an Ethernet switch. The host performing the capture must be attached to the same switch in the same VLAN as the PAA.

Cisco MDS 9000 SPAN Usage Instructions

On the Cisco MDS 9000 Family switch, traffic through any Fibre Channel interface can be replicated to an SD port. When a port is configured in SD mode, a copy of traffic (ingress, egress, or both) from a set of configured ports is sent to the SD port.

Tip Configure the extended inter-switch link (EISL) mode using the **switchport encap eisl** command if you need to debug or analyze VSAN-specific information.

Note For information on configuring the SPAN feature, see the *Cisco MDS 9000 Family CLI Configuration Guide*.

A valid Fibre Channel port on a Cisco MDS 9000 Family switch must be configured as an SD port. Once a Fibre Channel port is in SD port mode, it cannot be used for normal data traffic.

In SD port mode, the Fibre Channel port of the switch has the following characteristics:

- Packets are always output from the port (egress). The port never receives any frames.
- The port cannot be flow-controlled.
- No handshaking is performed.
- The receiving device does not need a Fibre Channel address.

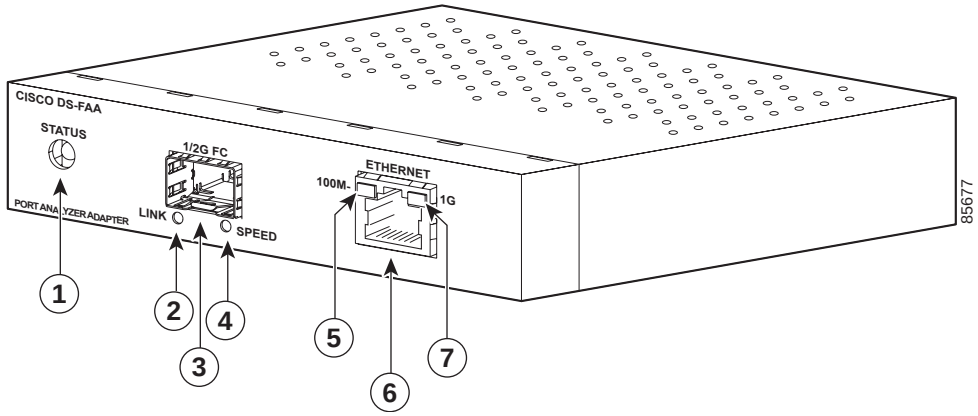
The following usage considerations apply to a PAA connected to a Cisco MDS 9000 Family switch:

- The adapter receives data only; the adapter does not transmit data to the switch.
- The LED on the Fibre Channel SD port on the switch cannot be used to diagnose a problem.

Hardware Description

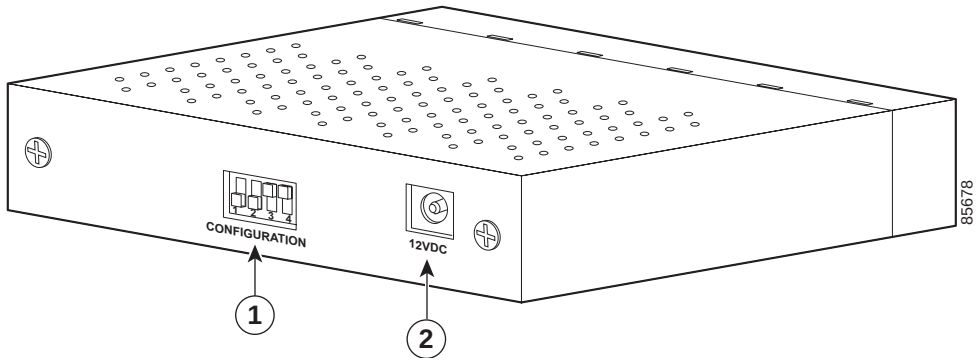
See the front view of the Port Analyzer Adapter in Figure 2and the rear view in Figure 3.

Figure 2 Cisco MDS 9000 Family Port Analyzer Adapter—Front View



1	Status LED	**5**	Ethernet LED for 100 Mbps
2	Fibre Channel Link LED	**6**	Ethernet port
3	Fibre Channel port	**7**	Ethernet LED for 1 Gbps
4	Fibre Channel Speed LED		

Figure 3 Cisco MDS 9000 Family Port Analyzer Adapter—Rear View



1	DIP switches	**2**	12-VDC power input

The four DIP switches, numbered 1 through 4 from left to right, are used to select the truncate mode as described in the “Modes of Operation” section on page 7.

LED Descriptions

The PAA has five LEDs on its faceplate (see Figure 2).

Table 1 lists the LEDs, their conditions, and what the conditions indicate.

Table 1 LED Descriptions

LED Type	Status	Description
Status	Off	Either the power to the adapter is off or there is a power failure. The adapter cannot power up.
	Red	Power is up, but there is some other failure. To attempt to fix the failure, power cycle the adapter by powering off and waiting for more than four seconds before powering on. To power cycle, disconnect the power cord from the wall rather than from the adapter.
	Green	The adapter is functioning correctly.
Fibre Channel Link	Off	The Fibre Channel link is down.
	Green	The Fibre Channel link is up.
Fibre Channel Speed	Off	The Fibre Channel link is programmed in 1-Gbps mode.
	Green	The Fibre Channel link is programmed in 2-Gbps mode.
100-Mbps Ethernet	Off	The Ethernet link is down. The link speed might not be negotiated. The LED is off when Ethernet is configured in 1-Gbps mode.
	Green	The Ethernet link is up in 100-Mbps mode.
	Blinking green	Ethernet frames are being transmitted on the Ethernet link.
1-Gbps Ethernet	Off	The Ethernet link is down. The link speed might not be negotiated. The LED is off when Ethernet is configured in 100-Mbps mode.
	Green	The Ethernet link is up in 1-Gbps mode.
	Blinking green	Ethernet frames are being transmitted on the Ethernet link.

Power Generation

The PAA requires 12-VDC external power. An AC converter is provided and connects to the power input at the rear of the unit.

Modes of Operation

The PAA has five modes of operation, four truncation modes and one no-truncate mode. These modes are used to configure the size of the frames that will be copied from the Fibre Channel interface. The two factors that are used to determine the setting are:

- The difference in speed of the Ethernet from the Fibre Channel interface.
- The amount of payload required for troubleshooting purposes.

This balance can be achieved by using one of the four truncate modes to increase or decrease the frame rate at the expense of reducing or increasing the payload. By truncating the Fibre Channel payload, the adapter can transmit more frames per second on the Ethernet interface.

There are four external DIP switches on the rear of the adapter, numbered 1 through 4, from left to right. These switches configure the PAA to operate at either 1-Gbps or 2-Gbps Fibre Channel speed in one of the five modes of operation.

The modes of operation are as follows:

- No truncate mode (NTM)
- Ethernet truncate mode (ETM)
- Shallow truncate mode (STM)
- Deep truncate mode (DTM)
- Management mode (MNM)

A speed mismatch between the Fibre Channel and the Ethernet side of the adapter could affect the frame throughput on the Ethernet side. For example, if the Fibre Channel speed is set at 2 Gbps, and the Ethernet speed is set at 1 Gbps, and all packets on the Fibre Channel side are 2164 bytes in size, you must configure the adapter to DTM or STM mode for the Ethernet side to receive all frames. If the adapter were in ETM (or NTM) mode, it would drop packets on the Ethernet side, and the Ethereal Network Analyzer might not see all the frames. Table 2 shows how the DIP switches should be configured for each Fibre Channel port speed and operating mode.

Table 2 DIP Switch Settings and Modes of Operation

Switch 1	Switch 2	Switch 3	Switch 4	Fibre Channel Mode	Operating Mode
ON	ON	ON	ON	1 Gbps	MNM
OFF	OFF	ON	ON	1 Gbps	DTM
OFF	ON	OFF	ON	1 Gbps	STM
ON	OFF	OFF	ON	1 Gbps	ETM
OFF	OFF	OFF	ON	1 Gbps	NTM
OFF	OFF	ON	OFF	2 Gbps	DTM
OFF	ON	OFF	OFF	2 Gbps	STM

Table 2 DIP Switch Settings and Modes of Operation (continued)

Switch 1	Switch 2	Switch 3	Switch 4	Fibre Channel Mode	Operating Mode
ON	OFF	OFF	OFF	2 Gbps	ETM
OFF	OFF	OFF	OFF	2 Gbps	NTM

Note The speed does not matter (1 or 2 Gbps) if you place a switch in MNM mode.

Caution Configuring a combination of DIP settings, other than those mentioned in Table 2, may have unpredictable consequences.

Truncate Mode

If you want to use truncate mode, you need the DS-PAA-2. DS-PAA does not support this.

The Cisco Traffic Analyzer's Fibre Channel throughput values are not accurate when used with the DS-PAA if data truncate is enabled. The DS-PAA-2 is required to achieve accurate results with truncate because it adds a count that enables the Cisco Traffic Analyzer to determine how many data bytes were actually transferred. By truncating a frame, you can push more packets through the PAA (2 Gbps for Fibre Channel to 1 Gbps or slower for Ethernet) and preserve privacy of the traffic being captured.

Selecting Truncate Mode

Note Truncate mode is available in DS-PAA version 2 and later.

Table 3 shows an example of how to select the truncate mode according to the average size of the Fibre Channel frame and the Fibre Channel-to-Ethernet speed. For example, with a 2164-byte Fibre Channel frame size, 1-Gbps Fibre Channel speed, and 100-Mbps Ethernet speed, you would select DTM mode.

Table 3 Selecting the Truncate Mode to Achieve No Dropped Frames

Average Size of the FC Frame	Fibre Channel to Ethernet Speed			
	1 Gbps to 1 Gbps	1 Gbps to 100 Mbps	2 Gbps to 1 Gbps	2 Gbps to 100 Mbps
2164 bytes (best case to obtain maximum data)	NTM, ETM, STM, or DTM	DTM	DTM or STM	DTM
1496 bytes	NTM, ETM, STM, or DTM	DTM	DTM or STM	Frames may be dropped.

Table 3 Selecting the Truncate Mode to Achieve No Dropped Frames (continued)

Average Size of the FC Frame	Fibre Channel to Ethernet Speed			
	1 Gbps to 1 Gbps	1 Gbps to 100 Mbps	2 Gbps to 1 Gbps	2 Gbps to 100 Mbps
512 bytes	NTM, ETM, STM, or DTM	Frames may be dropped.	DTM or STM	Frames may be dropped.
256 bytes (worst case to obtain maximum data)	NTM, ETM, STM, or DTM	Frames may be dropped.	DTM	Frames may be dropped.

The truncate modes can be hot switched (no power off is necessary). However, if you configure a new speed setting (for example, changing the Fibre Channel port speed from 2 Gbps to 1 Gbps), the adapter must be power cycled for the new setting to take effect. Power cycling consists of unplugging the adapter wall plug, waiting for four seconds or more, and then plugging it back in and powering on.

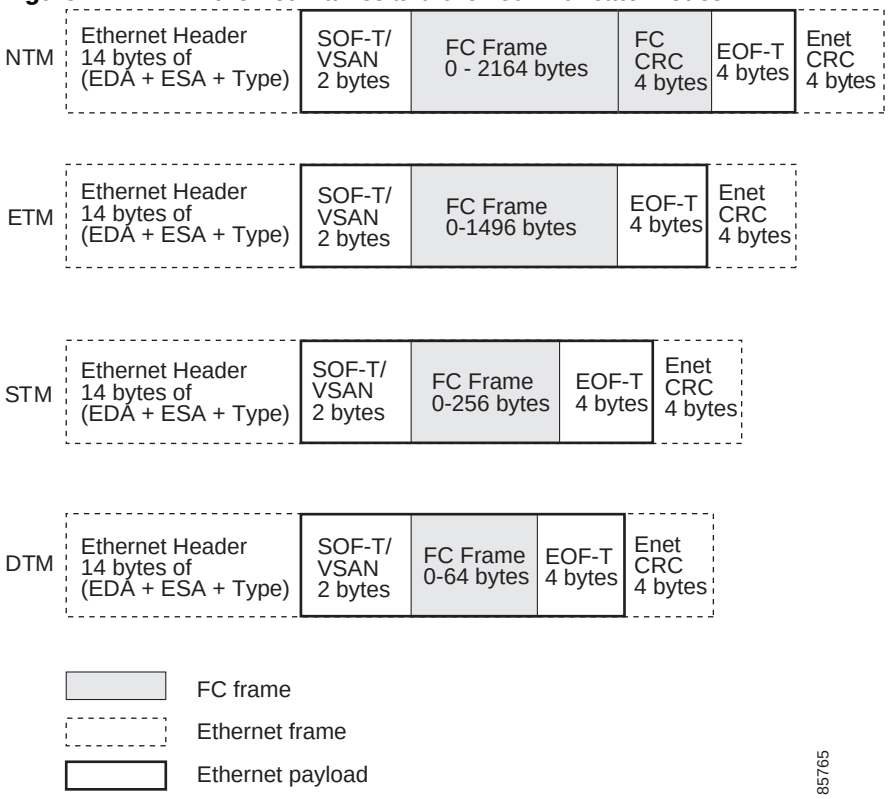
No Truncate Mode (NTM) for Ethernet Encapsulation

In NTM, Fibre Channel frames are encapsulated into Ethernet frames without any modification to the payload (the full 2164 bytes are transmitted). Ethernet devices must support jumbo frames for this mode to work; otherwise, the Ethernet MAC may not work properly for the frames larger than the maximum Ethernet size. Jumbo frames are Ethernet frames greater than 1520 bytes. (See Figure 4.)

Ethernet Truncate Mode (ETM) for Maximum Payload

This mode is appropriate when jumbo frames are not supported by the Ethernet devices. In that case, this mode provides the maximum amount of Fibre Channel payload within a single Ethernet frame.

Figure 4 Ethernet Frames and the Four Truncate Modes



In ETM, the adapter truncates a Fibre Channel frame to a maximum payload of 1496 bytes on the Ethernet side. Fibre Channel frames larger than 1496 bytes will be truncated. The Fibre Channel payload transmitted is 1472 bytes. (See Figure 4.)

Shallow Truncate Mode (STM)

STM provides less payload than ETM but more frames per second. In STM, the adapter truncates the Fibre Channel frame to 256 bytes. (See Figure 4.) Use this mode when you want more frames per second.

Deep Truncate Mode (DTM) for Most Frames per Second

As a default, the adapter comes configured in DTM mode and 1-Gbps Fibre Channel speed. This mode should be used when you want the most frames per second. DTM provides less payload than STM but more frames per second.

In DTM, the adapter truncates the Fibre Channel frame to 64 bytes. The total packet length including the Ethernet header and trailer is 88 bytes. (See Figure 4.)

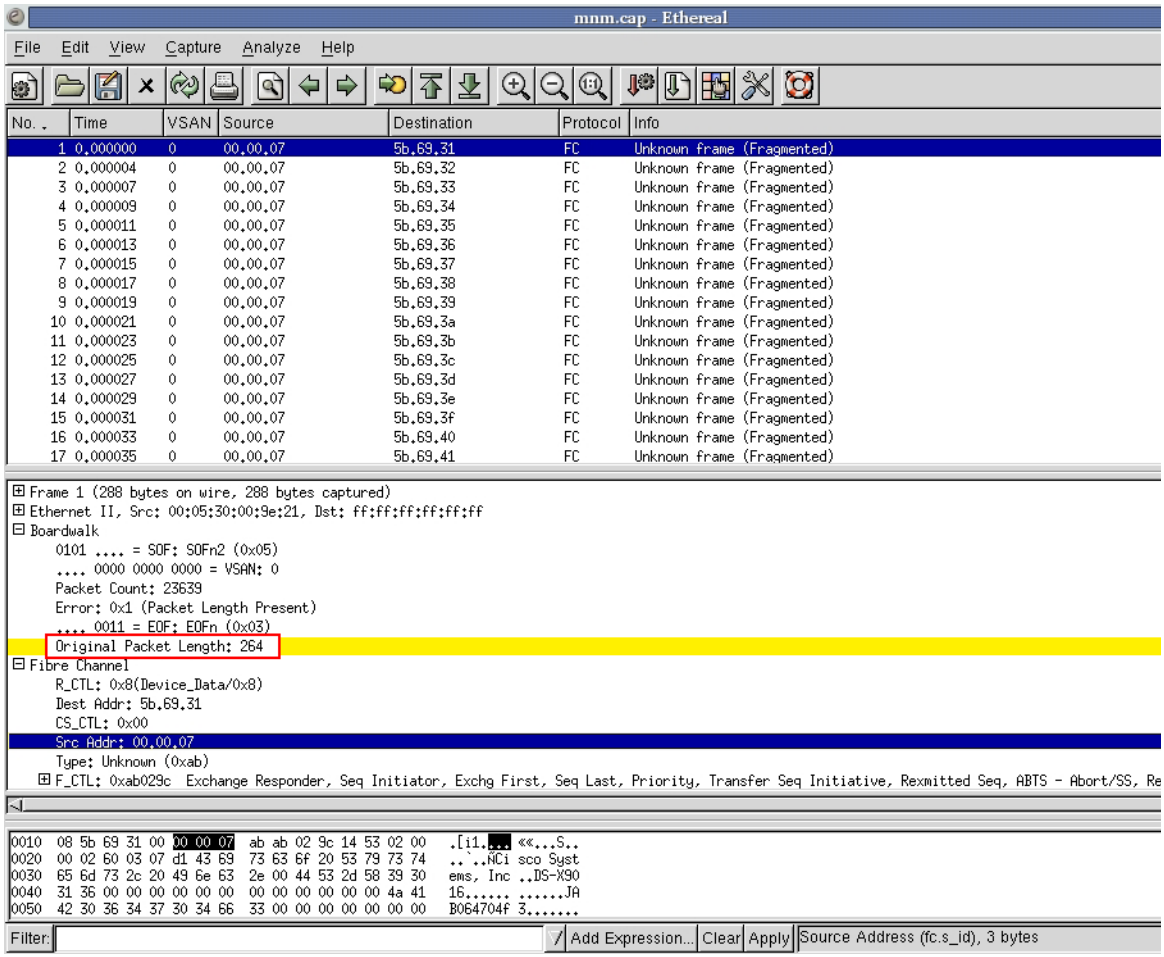
Management Mode (MNM) for Troubleshooting

MNM mode should be used only when troubleshooting the PAA. In this mode, the adapter will not accept any Fibre Channel frames.

In MNM, the adapter transmits a fixed 288-byte Ethernet frame that contains debug information for your use or for technical support calls. When calling technical support, also know the version number of the adapter . There are two versions of PAA, PAA-1 and PAA-2. If you see the **Original Packet Length** field in the debug information (highlighted in Figure 5), you are using a PAA-2. If this field is not present, you are using PAA-1.

Note The Cisco Traffic Analyzer must not be used with the PAA in MNM mode. The PAA in MNM mode generates traffic with perpetually changing host addresses; the Cisco Traffic Analyzer stores this redundant information and eventually runs out of memory.

Figure 5 Finding the PAA Version in Management Mode



The modes of operation are as follows:

- No truncate mode (NTM)
- Ethernet truncate mode (ETM)
- Shallow truncate mode (STM)
- Deep truncate mode (DTM)
- Management mode (MNM)

Installing the Port Analyzer Adapter

Note Before you install, operate, or service this equipment, read the *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family* for important safety information.

To install the Cisco MDS 9000 Family Port Analyzer Adapter, follow these steps:

Step 1 Configure the DIP switch settings at the rear of the adapter. See Table 2 on page 7 for DIP switch settings and modes of operation.

Step 2 Connect the AC power converter to the rear of the adapter.

Step 3 Connect the left (Fibre Channel) port on the adapter to the Fibre Channel SD port on the switch (see Figure 6). Use regular multimode fiber with LC to LC connectors (see Figure 7). Attach one LC connector to the switch and another LC connector to the adapter.

Figure 6 Connecting the Fibre Channel and Ethernet Ports

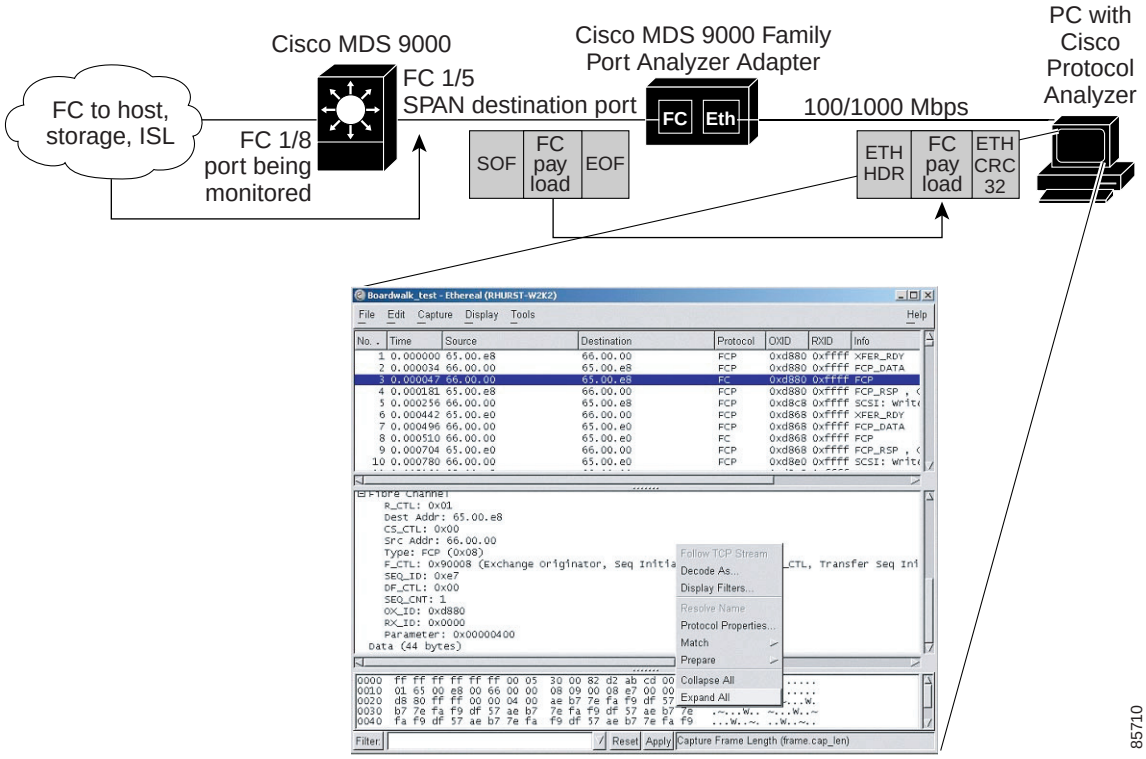
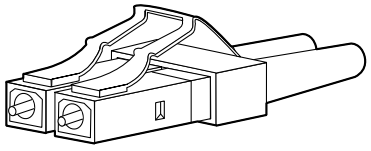


Figure 7 Multimode Fiber with LC Connector



Step 4 Connect the right (Ethernet) port on the adapter to the PC running Cisco Traffic Analyzer or Cisco Protocol Analyzer. If the NIC on your PC does not support auto-MDI, (1000baseT NICs generally support auto-MDI) you must use a crossover cable (see Figure 8) between the PAA and the PC. Otherwise, either a crossover or a straight-through Ethernet cable should work.

Table 4 lists the connector pinouts and signal names for straight-through cables that operate in Media-Dependent Interface (MDI) mode for Fast Ethernet ports.

Figure 8 Cross-over Cable for Connection to Ethernet Switch

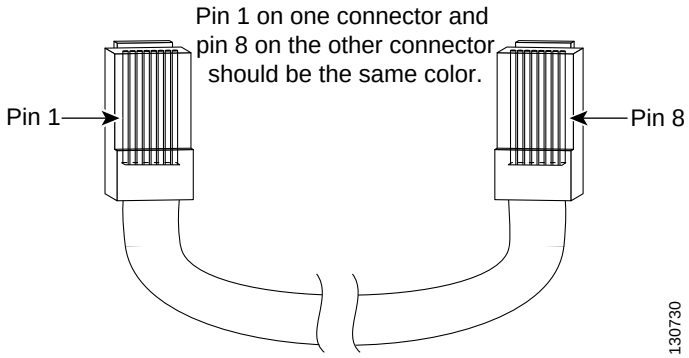


Table 4 Straight-Through Ethernet Cable Pinout (MDI)

RJ-45 Pin	Signal
1	Tx+
2	Tx–
3	Rx+
6	Rx–

Table 5 lists the connector pinouts and signal names for the cross-over cable.

Table 5 Cross-over Ethernet Cable Pinout

Cable End A		Cable End B	
RJ-45 Pin	**Signal**	**RJ-45 Pin**	**Signal**
1	Tx+	3	Rx+
2	Tx–	6	Rx–
3	Rx+	1	Tx+
6	Rx–	2	Tx–
4, 5, 7, 8	–	4, 5, 7, 8	–

Step 5 Verify that the LED states match the configured settings once the adapter has powered on. (See Table 1 on page 6 for the LED states.)

Troubleshooting the Port Analyzer Adapter

The front panel LEDs are the quickest way to evaluate the adapter operation.

Fibre Channel LED Not On

If the green Fibre Channel LED is not on, check to see if the GBIC is fully inserted. Try removing and reinstalling the GBIC. See the appropriate Cisco MDS hardware installation guide for installation of the required chassis.

Ethernet Link LED Not Blinking

If the Fibre Channel link is up but the Ethernet link LED is not blinking, do the following:

- Verify that the SD port and the adapter are configured to be the same speed.
- Verify that the SD port is sending out Fibre Channel frames by looking at the SPAN interface counter.

Setting Up the Cisco Traffic Analyzer

The Cisco Traffic Analyzer provides real-time analysis of SPAN traffic or analysis of captured traffic through a web browser user interface. Traffic encapsulated by one or more adapters can be analyzed concurrently with a single PC running nTop software, which is public domain software enhanced by Cisco for Fibre Channel traffic analysis.

This traffic analysis solution enables throughput to be determined for traffic between specific Fibre Channel sources and destinations, for all traffic in a particular virtual SAN (VSAN), or for all SPAN traffic. The following information is provided: round trip response times, SCSI I/Os per second, SCSI read versus write traffic throughput and frame counts, and SCSI session status and management task information. Additional statistics are also available on Fibre Channel frame sizes and network management protocols.

For seamless performance analysis and troubleshooting, launch the Cisco Traffic Analyzer in-context from Cisco Fabric Manager. Port world wide name (pWWN), Fibre Channel ID (FC ID), FC alias, and VSAN names are then passed to the Cisco Traffic Analyzer.

Note Accessing Cisco Traffic Analyzer changed with Fabric Manager Release 2.1(2). You can still run Cisco Traffic Analyzer from Fabric Manager Web Services. However, with Fabric Manager Release 2.1(2) or later, you can no longer access Cisco Traffic Analyzer from the Fabric Manager Client. For more information on releases prior to Fabric Manager Release 2.1(2), see the "Discovering Cisco Traffic Analyzer from Fabric Manager Web Services" section on page 20.

The nTop software runs on a host, such as a PC or workstation running Windows or Linux. This software, which supports VSANs and Fibre Channel decoding through the adapter, includes enhancements provided by Cisco to the public domain.

Note See the *Cisco MDS 9000 Family Fabric Manager Configuration Guide* for information about launching the Cisco Traffic Analyzer from the Performance Manager details charts. Performance Manager is a part of the Fabric Manager and is a licensed feature in Cisco SAN-OS Release 1.3(2a) or later.

Caution If data truncate is enabled, the Cisco Traffic Analyzer's Fibre Channel throughput values are not accurate when used with DS-PAA. The PAA version is required to achieve accurate results with truncate because it adds a count that enables the Cisco Traffic Analyzer to determine how many data bytes were actually transferred.

Tip You can use SPAN to monitor traffic on an interface without any traffic disruption. This feature is useful in troubleshooting scenarios when traffic disruption changes the problem environment and makes it difficult to reproduce the problem. See either the *Cisco MDS 9000 Family Fabric Manager Configuration Guide* or the *Cisco MDS 9000 Family CLI Configuration Guide*.

Caution The Cisco Traffic Analyzer must not be used with the PAA in MNM mode.

Using Cisco Traffic Analyzer with Fabric Manager Web Services

You can run Cisco Traffic Analyzer from within Fabric Manager Web Services in Fabric Manager Release 2.1(2) or later.

Note As of Fabric Manager Release 2.1(2) and later, you can no longer access Cisco Traffic Analyzer from Fabric Manager Client. However, you can still run Cisco Traffic Analyzer from Fabric Manager Web Services. For more information on releases prior to Fabric Manager Release 2.1(2), see the "Configuring Cisco Traffic Analyzer for Fabric Manager Releases Prior to 2.1(2)" section on page 21.

This section includes the following topics:

Installing Cisco Traffic Analyzer

You must launch Cisco Traffic Analyzer before you can discover and access it from Fabric Manager Web Services. At a minimum, you need to provide the directory where Cisco Traffic Analyzer stores its database, including the RRD files that it creates for trending.

Note Do not use the /tmp directory for storing the Cisco Traffic Analyzer database on UNIX or Linux workstations. Many distributions of Linux periodically clean up the /tmp directory, thereby affecting Cisco Traffic Analyzer. Instead you can use the /var/ntop directory.

Verify that you have sufficient space in the partition where the Cisco Traffic Analyzer database is stored.

To install and launch Cisco Traffic Analyzer on a UNIX workstation, follow these steps:

Step 1 Open a browser and go to the following website to access the web page where Cisco Traffic Analyzer is available:
http://cisco.com/cgi-bin/tablebuild.pl/mds-fm.

Step 2 Download fc-ntop.tar.gz and install it using the instructions at the following website:
http://www.ntop.org.

Step 3 Launch nTop using the following UNIX command:

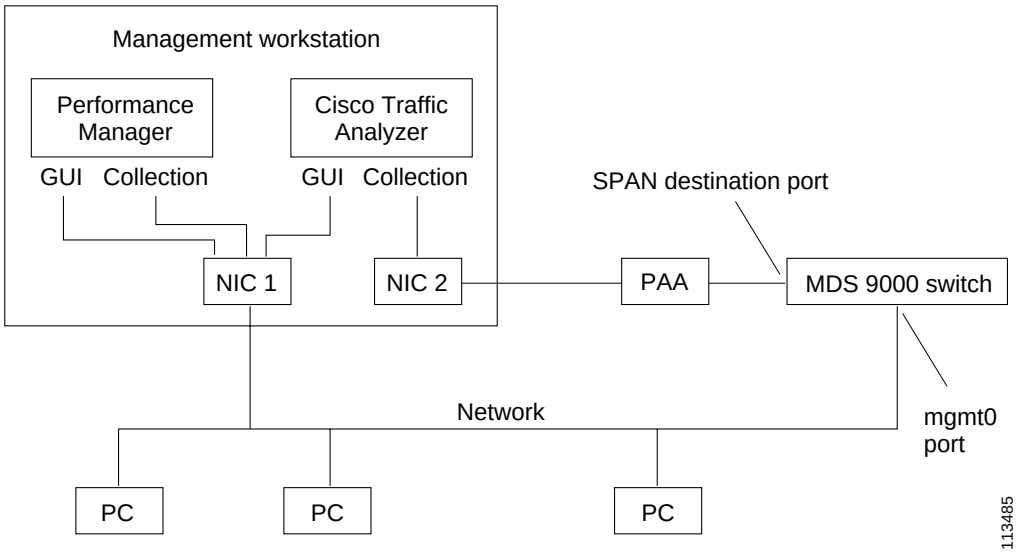
```
ntop -P database_directory
```

where *database_directory* is the directory where you want Cisco Traffic Analyzer to save its database files (for example, /var/ntop).

Note If another application uses port 3000, you can change the port that Cisco Traffic Analyzer uses by entering the following in Step 3:
ntop.exe /c -P tmp -w *port_number*, where *port_number* is equal to the port that you want Cisco Traffic Analyzer to use. Set the port number to 3001 if you want to use SSL. Fabric Manager Web Services can only detect Cisco Traffic Analyzer if you use port 3000 (the default port).

Step 4 Verify that the Fibre Channel port on the PAA is connected to the SD port on the switch (see Figure 9).

Figure 9 Fibre Channel Port on the PAA connected to an SD Port



Step 5 Verify that the Ethernet port on the PAA is connected to the workstation running Cisco Traffic Analyzer.

Step 6 Click **Interfaces > SPAN...** in Device Manager to configure SPAN on the required switch ports.

Step 7 Click **Interfaces > SPAN...** in Device Manager to verify that the Fibre Channel port connected to the PAA is configured as an SD port. The port mode of the destination interface must be SD.

Step 8 Click the **Sessions** tab in Device Manager to verify the correct destination and source of traffic (ingress).

In Windows, you can use the \tmp directory provided with the distribution to store the Cisco Traffic Analyzer database.

To install and launch Cisco Traffic Analyzer on a Windows workstation, follow these steps:

Step 1 Open a browser and go to the following website to access the web page where Cisco Traffic Analyzer is available:
http://cisco.com/cgi-bin/tablebuild.pl/mds-fm.

Step 2 Download ntop-win32.zip and save it on your workstation.

Step 3 Unzip the downloaded file.

Note You need the WinPcap version 3.1 or later library file to use Cisco Traffic Analyzer on a Microsoft Windows system. You can download this file from the Cisco CD that shipped with your product, or from the following website:
http://winpcap.polito.it/.

Step 4 Open a command prompt and change directories to your nTop installation directory.

Step 5 Enter **ntop.exe /c -P *database_directory*** or install nTop as a service on Windows by following these steps:

a. Enter **ntop /i** to install nTop as a service.

b. Choose **Start > Programs > Administrative Tools > Services** to access the Windows Services Panel.

c. Right-click **nTop** and choose **properties**. You see the Properties dialog box.

d. Set the Start Parameters to -P ***database_ directory,*** where *database_directory* is the directory where you want Cisco Traffic Analyzer to store its database (for example, D:\ntop\tmp).

Note If launching Cisco Traffic Analyzer as a Windows service, you must specify the complete path for the database directory using the -P option.

Note If another application uses port 3000, you can change the port that Cisco Traffic Analyzer uses by entering the following in Step 5:
ntop.exe /c -P tmp -w *port_number*, where *port_number* is equal to the port that you want Cisco Traffic Analyzer to use. Set the port number to 3001 if you want to use SSL. Fabric Manager Web Services can only detect Cisco Traffic Analyzer if you use port 3000 (the default port).

e. Click **Start** to start nTop on that interface.

Note Subsequent restarts of the nTop service do not require setting the -i option, unless you are changing the interface that connects to the PAA.

Step 6 Optionally, choose **Admin > Startup Preferences > Capture** to set the interface that Cisco Traffic Analyzer uses after Cisco Traffic Analyzer opens.

Step 7 Select the interfaces that are receiving PAA traffic that Cisco Traffic Analyzer will capture packets on.

Step 8 Verify that the Fibre Channel port on the PAA is connected to the SD port on the switch (see Figure 9).

Step 9 Verify that the Ethernet port on the PAA is connected to the workstation running Cisco Traffic Analyzer.

Step 10 Click **Interfaces > SPAN...** in Device Manager to configure SPAN on the required switch ports.

Step 11 Click the **Sources** tab in Device Manager to verify that the Fibre Channel port connected to the PAA is configured as an SD port. The port mode of the destination interface must be SD.

Step 12 Click the **Sessions** tab in Device Manager to verify the correct destination and source of traffic (ingress).

Tip To modify the script that launches nTop (ntop.sh or ntop.bat), follow the instructions provided within the script file. Create a backup of the original script before modifying the file.
—Linux platforms use the shell script path. The nTop output is sent to the syslog file (/var/log/messages by default).
—Windows platforms use the batch file. The nTop output is sent to a file located in the same directory as the one from which nTop is launched.

You can remove Cisco Traffic Analyzer as a service by entering the following command at the Windows command prompt:

```
ntop.exe /r
```

Launching Cisco Traffic Analyzer

To access an instance of Cisco Traffic Analyzer running in your fabric from Fabric Manager Web Services, follow these steps:

Step 1 Choose **Performance > Traffic Analyzer**. You see a summary table of all SPAN destination ports and configured Cisco Traffic Analyzers in your fabric. The source column shows the ports that are monitored by the SPAN destination port.

Step 2 Click the Cisco Traffic Analyzer that connects to the SPAN port you want to monitor to launch that Cisco Traffic Analyzer within Fabric Manager Web Services.

To launch the Cisco Traffic Analyzer outside Fabric Manager, follow these steps:

Step 1 Change to the directory where the Cisco Traffic Analyzer is installed and run the script file. For example, if you have installed nTop under /usr/local on Linux, type this:

```
cd /usr/local/fc-ntop
sh -x ntop.sh
```

Step 2 Access the nTop URL by typing http://localhost:3000 in the Address field of your web browser.

Tip To modify the script that launches nTop (ntop.sh or ntop.bat), follow the instructions provided within the script file. Create a backup of the original script before modifying the file.
—Linux platforms use the shell script path. The nTop output is sent to the syslog file (/var/log/messages by default).
—Windows platforms use the batch file. The nTop output is sent to a file located in the same directory as the one from which nTop is launched.

Discovering Cisco Traffic Analyzer from Fabric Manager Web Services

Fabric Manager Release 2.1(2) or later supports discovering instances of Cisco Traffic Analyzer and SPAN ports configured within your fabric from Fabric Manager Web Services.

Fabric Manager Web Services supports the following Traffic Analyzer integration features:

- SCSI I/O Traffic Analyzer pages can be viewed within the Web client.
- Traffic Analyzer can reside on a different server than Performance Manager.
- Performance Manager integrates with multiple servers running Traffic Analyzer.
- Instances of Traffic Analyzer servers can be discovered by Fabric Manager Server.
- Web client report lists SPAN destination ports and associations with Traffic Analyzers.

To discover instances of Traffic Analyzer running in your fabric from Fabric Manager Web Services, follow these steps:

Step 1 Choose **Performance > Traffic Analyzer**. You see a summary table of all SPAN destination ports and configured Traffic Analyzers in your fabric.

Step 2 Navigate to the fabric where you want to rediscover instances of Traffic Analyzer from the navigation bar.

Step 3 Set Search on Subnet to the subnet that you want to rediscover.

Step 4 Click **Rediscover** to find instances of Traffic Analyzer within the selected fabric or VSAN and subnet.

Note Fabric Manager Web Services can only detect instances of Traffic Analyzer that use port 3000.

Accessing Cisco Traffic Analyzer from Fabric Manager Web Services

To access an instance of Cisco Traffic Analyzer running in your fabric from Fabric Manager Web Services, follow these steps:

Step 1 Choose **Performance > Traffic Analyzer**. You see a summary table of all SPAN destination ports and configured Traffic Analyzers in your fabric. The source column shows the ports that are monitored by the SPAN destination port.

Step 2 Click a Traffic Analyzer to launch that Traffic Analyzer within Fabric Manager Web Services.

If you did not configure the switch and switch port information in Cisco Traffic Analyzer, you can still discover it, but Fabric Manager Web Services cannot associate that instance of Cisco Traffic Analyzer with any fabric. Cisco Traffic Analyzer also cannot inherit the device alias information from Fabric Manager Web Services.

Fabric Manager Web Services updates Cisco Traffic Analyzer with the latest device alias information every five minutes.

Configuring Cisco Traffic Analyzer for Fabric Manager Releases Prior to 2.1(2)

To configure Performance Manager to work with Cisco Traffic Analyzer for Fabric Manager releases prior to Release 2.1(2), follow these steps:

Step 1 Get the following three pieces of information:

- The IP address of the management workstation on which you are running Performance Manager and Cisco Traffic Analyzer.
- The path to the directory where Cisco Traffic Analyzer is installed.
- The port that is used by Cisco Traffic Analyzer (the default is 3000).

Step 2 Start Cisco Traffic Analyzer.

a. Choose **Performance > Traffic Analyzer > Open**.

b. Enter the URL for Cisco Traffic Analyzer, in the format

`http://ip_address:port_number`

where *ip_address* is the address of the management workstation on which you have installed the Cisco Traffic Analyzer, and :*port_number* is the port that is used by Cisco Traffic Analyzer (the default is :3000).

c. Click **OK**.

d. Choose **Performance** > **Traffic Analyzer** > **Start**.

e. Enter the location of Cisco Traffic Analyzer, in the format

`D:directory\ntop.bat`

where D: is the drive letter for the disk drive where Cisco Traffic Analyzer is installed, and *directory* is the directory containing the ntop.bat file.

f. Click **OK**.

Step 3 Create the flows you want Performance Manager to monitor using the Flow Configuration Wizard.

Step 4 Define the data collection you want Performance Manager to gather using the Performance Manager Configuration Wizard.

a. Choose the VSAN you want to collect information for or choose **All VSANs**.

b. Check the types of items you want to collect information for (hosts, ISLs, storage devices, and flows).

c. Enter the URL for Cisco Traffic Analyzer in the format

`http://ip address/directory`

where *ip address* is the address of the management workstation on which you have installed Cisco Traffic Analyzer, and *directory* is the path to the directory where Cisco Traffic Analyzer is installed.

d. Click **Next**.

e. Review the end devices and links that you selected to make sure this is the data you want to collect.

f. Click **Finish** to begin collecting data.

Note Data is not collected for JBODs or for virtual ports. If you change the data collection configuration parameters during a data collection, you must stop and restart the collection process for your changes to take effect.

Step 5 Click **Cisco Traffic Analyzer** at the top of the Host or Storage detail pages to view Cisco Traffic Analyzer information, or choose **Performance** > **Traffic Analyzer** > **Open**. Cisco Traffic Analyzer will not open unless nTop has been started already.

Setting Up the Cisco Protocol Analyzer

The Cisco Protocol Analyzer enables Fibre Channel traffic to be analyzed at the frame level in real-time or from captured SPAN traffic through a graphical user interface. Traffic encapsulated by an adapter can be analyzed by Ethereal, a public domain software enhanced by Cisco for Fibre Channel and SCSI protocol decoding.

Ethereal can analyze traffic from a single adapter at a time when running on Microsoft Windows, but it can capture and analyze aggregate traffic from multiple adapters when running on Linux. Ethereal filters captured data to reduce file size, and it filters the information displayed so that it is easy to locate the frames of greatest interest. Its unique ability to match Fibre Channel requests and responses greatly simplifies analysis and searching for detailed information, including response times. Ethereal has also been enhanced to be VSAN aware.

The Ethereal software runs on a host, such as a PC or workstation running Windows or Linux. This software, which supports VSAN and Fibre Channel decoding through the adapter, includes enhancements provided by Cisco to the public domain.

Download the latest version of Ethereal from http://www.ethereal.com. If you need to perform remote captures, use the version provided at the Cisco Software Center.

Note When performing remote captures in a Linux environment, be aware that the **Update List of Packets in Real time** option in the capture dialog box cannot be enabled, and the packet count may not be displayed even though packets are received.

To install the Ethereal software on a PC with the Windows operating system, follow these steps:

Step 1 Download the Ethereal software from the web and follow the instructions for installing it.

Step 2 Verify that the left (Fibre Channel) port on the adapter is connected to the SD port on the switch. (See Figure 9.)

Step 3 Verify that the right (Ethernet) port on the adapter is connected to the PC running the Ethereal software.

Step 4 Configure SPAN on the required Cisco MDS 9000 ports.

Step 5 Verify that the Fibre Channel port connected to the adapter is configured as an SD port by using the **show interface** command. See the *Cisco MDS 9000 Family CLI Configuration Guide*. The port mode of the destination interface must be SD.

Step 6 Verify the correct destination and source of traffic (ingress) by using the **show span session** command. See the *Cisco MDS 9000 Family CLI Configuration Guide*.

Creating Display Filters

You can selectively view captured frames by using the display filters feature. For example, instead of viewing all the frames from a capture, you may want to view only ELP request frames. This feature limits the captured view only—it does not affect the captured or the saved frames. Procedures to specify, use, and save display filters are already documented at the following website under MDS 9000 Family software: http://www.cisco.com/kobayashi/sw-center/sw-stornet.shtml. Click **Cisco MDS 9000 Family Port Analyzer Adapter** to view the filters. The following list includes examples of ways to use this feature:

- To view all packets in a specified VSAN, use this expression:

  ```
  mdshdr.vsan == 2 || brdwlk.vsan == 2
  ```

- To view all SW_ILS frames, use this expression:

  ```
  fcswils
  ```

- To view class F frames, use this expression:

  ```
  mdshdr.sof == SOFf || brdwlk.sof == SOFf
  ```

- To view all FSPF frames, use this expression:

  ```
  swils.opcode == JLO || swils.opcode == LSU || swils.opcode == LSA
  ```

- To view all FLOGI frames, use this expression:

  ```
  fcels.opcode == FLOGI
  ```

- To view all FLOGI frames in VSAN 2, use this expression:

  ```
  fcels.opcode == FLOGI && (mdshdr.vsan == 2 || brdwlk.vsan == 2)
  ```

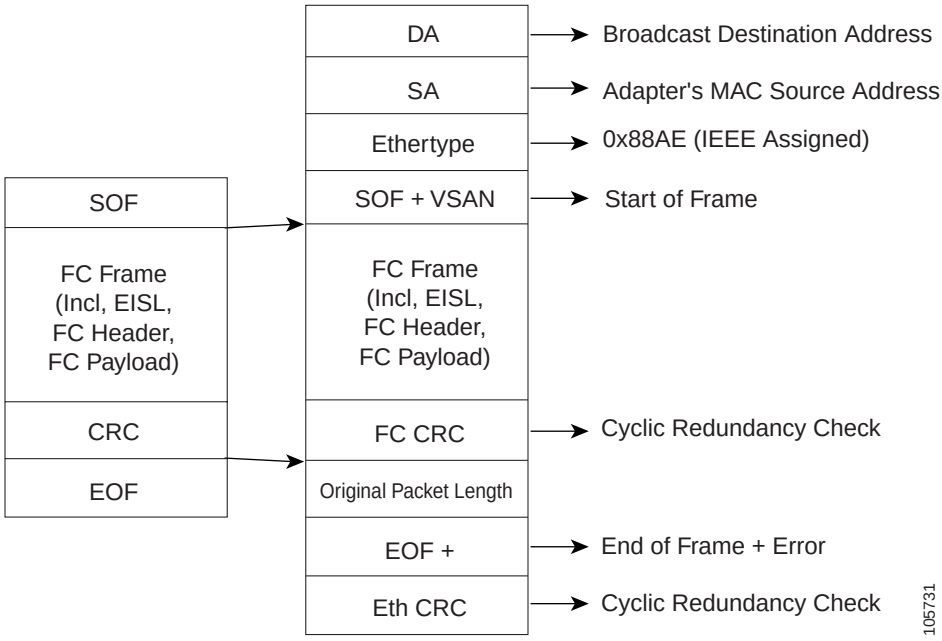
- To view all name server frames, use this expression:

  ```
  dNS
  ```

Ethernet Frame Addressing Format

This section describes fields in the Ethernet frame, after the adapter encapsulates the Fibre Channel frame into an Ethernet frame. (See Figure 10.)

Figure 10 Fibre Channel Encapsulation



The following list shows the fields of an Ethernet frame:

- Ethernet Destination Address—The 6-byte MAC address for the frame destination. A broadcast EDA (FF:FF:FF:FF:FF:FF) is used and cannot be changed.
- Ethernet Source Address—The 6-byte MAC address of the Ethernet port. It cannot be changed. The source address is burned in at the factory.
- Ethertype field—This field has the value 0x88AE.
- Original packet length—The original packet length is measured in words and is a minimum of 12 words (36 bytes) and a maximum of 528 words (2112 bytes).

Related Documentation

The documentation set for the Cisco MDS 9000 Family includes the following documents. To find a document online, use the Cisco MDS SAN-OS Documentation Locator at:

http://www.cisco.com/en/US/products/ps5989/products_documentation_roadmap09186a00804500c1.html.

For information on IBM TotalStorage SAN Volume Controller Storage Software for the Cisco MDS 9000 Family, refer to the IBM TotalStorage Support website:

http://www.ibm.com/storage/support/2062-2300/

Release Notes

- *Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Releases*
- *Cisco MDS 9000 Family Release Notes for Storage Services Interface Images*
- *Cisco MDS 9000 Family Release Notes for Cisco MDS SVC Releases*
- *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images*

Compatibility Information

- *Cisco MDS 9000 SAN-OS Hardware and Software Compatibility Information*
- *Cisco MDS 9000 Family Interoperability Support Matrix*
- *Cisco MDS SAN-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for*
- *Cisco MDS 9000*
- *Cisco MDS SAN-OS Release Compatibility Matrix for Storage Service Interface Images*

Regulatory Compliance and Safety Information

- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*

Hardware Installation

- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9216 Switch Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9020 Fabric Switch Hardware Installation Guide*

Send documentation comments to mdsfeedback-doc@cisco.com.

Cisco Fabric Manager

- *Cisco MDS 9000 Family Fabric Manager Quick Configuration Guide*
- *Cisco MDS 9000 Family Fabric Manager Configuration Guide*
- *Cisco MDS 9000 Fabric Manager Online Help*
- *Cisco MDS 9000 Fabric Manager Web Services Online Help*

Command-Line Interface

- *Cisco MDS 9000 Family Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family CLI Quick Configuration Guide*
- *Cisco MDS 9000 Family CLI Configuration Guide*
- *Cisco MDS 9000 Family Command Reference*
- *Cisco MDS 9000 Family Quick Command Reference*
- *Cisco MDS 9020 Fabric Switch Configuration Guide and Command Reference*
- *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*

Troubleshooting and Reference

- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family MIB Quick Reference*
- *Cisco MDS 9020 Fabric Switch MIB Quick Reference*
- *Cisco MDS 9000 Family CIM Programming Reference*
- *Cisco MDS 9000 Family System Messages Reference*
- *Cisco MDS 9020 Fabric Switch System Messages Reference*

Installation and Configuration Note

- *Cisco MDS 9000 Family SSM Configuration Note*
- *Cisco MDS 9000 Family Port Analyzer Adapter Installation and Configuration Note*

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Send documentation comments to mdsfeedback-doc@cisco.com.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

Send documentation comments to mdsfeedback-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Printed in the USA on recycled paper containing 10% postconsumer waste.

Send documentation comments to mdsfeedback-doc@cisco.com.