



Advanced Features and Concepts

This chapter describes the advanced features provided in switches in the Cisco MDS 9000 Family. It includes the following sections:

This chapter contains the following topics:

- [Configuring FC Timers, page 31-1](#)
- [Configuring a Fabric Analyzer, page 31-2](#)
- [Configuring World Wide Names, page 31-5](#)
- [Allocating Flat FC IDs, page 31-5](#)
- [Enabling Loop Monitoring, page 31-6](#)
- [Configuring the Switch for Interoperability, page 31-6](#)
- [Using the show tech-support Command, page 31-8](#)
- [Managing World Wide Names, page 31-9](#)
- [Configuring Timers, page 31-9](#)

Configuring FC Timers

The **ftimer** command modifies Fibre Channel protocol related timer values for the switch.

You can use the **ftimer** command in configuration mode to configure the following TOVs:

- Distributed services TOV (D_S_TOV)—The valid range is from 5,000 to 10,000 milliseconds. The default is 5,000 milliseconds.
- Error detect TOV (E_D_TOV)—The valid range is from 1,000 to 10,000 milliseconds. The default is 2,000 milliseconds. This value is matched with the other end during port initialization.
- Resource allocation TOV (R_A_TOV)—The valid range is from 5,000 to 10,000 milliseconds. The default is 10,000 milliseconds. This value is matched with the other end during port initialization.



Note

The Fabric stability TOV (F_S_TOV) constant cannot be configured.

Configuring Timers Per-VSAN

You can also issue the **ftimer** command for a specified VSAN to configure different TOV values for VSANs with special links like FC or IP tunnels. You can configure different E_D_TOV, R_A_TOV, and D_S_TOV values for individual VSANs. Active VSANs are suspended or activated when their timer values are changed.

**Caution**

You cannot perform a nondisruptive downgrade to any earlier version which does not support per-VSAN FC timers.

**Note**

This configuration must be propagated to all switches in the fabric--be sure to configure the same value in all switches in the fabric.

If a switch is downgraded to SAN-OS Release 1.2(x) or 1.1(x) after the timer is configured for a VSAN, an error message is issued to warn the user about strict incompatibilities. Refer to the Cisco MDS 9000 Family Troubleshooting Guide for further information.

Configuring a Fabric Analyzer

Fibre Channel protocol analyzers capture, decode, and analyze frames and ordered sets on a link. While existing Fibre Channel analyzers can capture traffic at wire rate speed. They are expensive and support limited frame decoding. Also, to snoop traffic, the existing analyzers disrupt the traffic on the link while the analyzer is inserted into the link.

Cisco has brought protocol analysis within a storage network to a new capability level with the Cisco Fabric Analyzer. You can capture Fibre Channel control traffic from a switch and decode it without having to disrupt any connectivity, and without having to be local to the point of analysis.

The Cisco Fibre Channel protocol analyzer is based on two popular public-domain software applications:

- libpcap—You can obtain more information from <http://www.tcpdump.org>.
- Ethereal—You can obtain more information from <http://www.ethereal.com>.

**Note**

The Cisco Fabric Analyzer is useful in capturing and decoding control traffic, not data traffic. It is suitable for control path captures, and is not intended for high-speed data path captures.

This section explains the following topics:

This section contains the following topics:

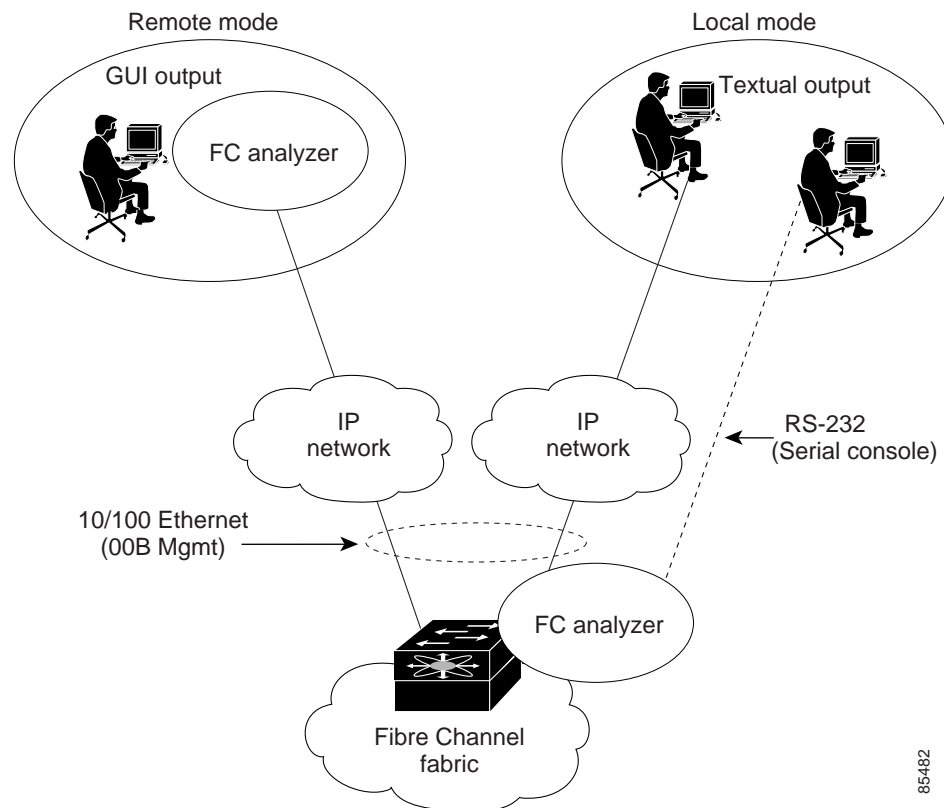
- [About the Cisco Fabric Analyzer, page 31-3](#)
- [Configuring the Cisco Fabric Analyzer, page 31-4](#)

About the Cisco Fabric Analyzer

The Cisco Fabric Analyzer comprises two separate components:

- A software that runs on the Cisco MDS 9000 Family switch and supports two modes of capture:
 - a text-based analyzer that supports local capture and decodes captured frames
 - a daemon that supports remote capture
- A GUI-based client that runs on a host that supports libpcap such as Windows or Linux and communicates with the remote capture daemon in a Cisco MDS 9000 Family switch.

Figure 31-1 Cisco Fabric Analyzer Usage



Local Text-Based Capture

This component is a command-line driven text-based interface that captures traffic to and from the supervisor module in a Cisco MDS 9000 switch. It is a fully-functional decoder that is useful for quick debug purposes or for use when the remote capture daemon is not enabled. Additionally, because this tool is accessed from within the Cisco MDS 9000 switch, it is protected by the roles-based policy that limits access in each switch.

Remote Capture Daemon

This daemon is the server end of the remote capture component. The Ethereal analyzer running on a host is the client end. They communicate with each other using the Remote Capture Protocol (RPCAP). RPCAP uses two end points, a TCP-based control connection and a TCP or UDP-based data connection based on TCP (default) or UDP. The control connection is used to remotely control the captures (start or stop the capture, or specify capture filters). Remote capture can only be performed to explicitly configured hosts. This technique prevents unauthorized machine in the network from snooping on the control traffic in the network.

RPCAP supports two setup connection modes based on fire wall restrictions.

- **Passive mode (default)**—The configured host initiates connection to the switch. Multiple hosts can be configured to be in passive mode and multiple hosts can be connected and receive remote captures at the same time.
- **Active mode**—The switch initiates the connection to a configured host—one host at a time.

Using capture filters, you can limit the amount of traffic that is actually sent to the client. Capture filters are specified at the client end--on Ethereal, not on the switch.

GUI-Based Client

The Ethereal software runs on a host, such as a PC or workstation, and communicates with the remote capture daemon. This software is available in the public domain from <http://www.ethereal.com>. Since Ethereal has a GUI front-end, it supports a rich functionality such as colorized display, graphical assists in defining filters, and searching for specific frames. These features are documented on the Ethereal web site.

While remote capture via Ethereal supports capturing and decoding Fibre Channel frames from a Cisco MDS 9000 Family switch, the host running Ethereal does not require a Fibre Channel connection to the switch. The remote capture daemon running on the switch sends the captured frames over the out-of-band Ethernet management port. This capability allows you to capture and decode Fibre Channel frames from your desktop or laptop.

Configuring the Cisco Fabric Analyzer

You can configure the Cisco Fabric Analyzer by issuing the **fcanalyzer local** or **fcanalyzer remote** commands in configuration mode.

- **Local capture**—The command setting to enable a local capture cannot be saved to persistent storage or synchronized to standby.
- **Remote capture**—The command setting to enable a remote capture can be saved to persistent storage using the **copy** command. It can be synchronized to the standby supervisor module and a stateless restart can be issued, if required.

To use the Cisco Fabric Analyzer feature, traffic should be flowing to or from the supervisor module.

Configuring World Wide Names

The world wide name (WWN) in the switch is equivalent to the Ethernet MAC address. As with the MAC address, you must uniquely associate the WWN to a single device. The principal switch selection and the allocation of domain IDs rely on the WWN. The WWN manager, a process-level manager residing on the switch supervisor module, assigns WWNs to each switch. This WWN is independent of other WWNs on each switch. This centralized control of WWN has the following advantages:

- Efficient sharing of WWN space
- Centralized support across switches

Cisco MDS 9000 Family switches support three network address authority (NAA) address formats.

Table 31-1 Standardized NAA WWN Formats

NAA Address	NAA Type	WWN Format	
IEEE 48-bit address	Type 1 = 0001b	000 0000 0000b	48-bit MAC address
IEEE extended	Type 2 = 0010b	Locally assigned	48-bit MAC address
IEEE registered	Type 5 = 0101b	IEEE company ID: 24 bits	VSID: 36 bits



Caution

Changes to the worldwide names should be made by an administrator or individual who is completely familiar with switch operations.

Allocating Flat FC IDs

Fibre Channel standards require a unique FC ID to be allocated to a N port attached to a Fx port in any switch. To conserve the number of FC IDs used, Cisco MDS 9000 Family switches use a special allocation scheme.

Based on the assigned FC ID, some HBAs assume that no other ports have the same area bits and domain. When a target is assigned with a FC ID that has the same area bits, but different port bits, the HBA fails to discover these targets. To isolate these HBAs in a separate area, switches in the Cisco MDS 9000 Family follow a different FC ID allocation scheme. By default, the FC ID allocation mode is **auto**. In the **auto** mode, only HBAs without interop issues are assigned FCIDs with specific ports bits. All other HBAs are assigned FC IDs with a whole area (port bits set to 0).

The three options to allocate FCID are auto (default), none, and flat.



Caution

Changes to FC IDs should be made by an administrator or individual who is completely familiar with switch operations.

Enabling Loop Monitoring

When a disk is removed from a loop port, the loop stays active based on the bypass circuit. Thus the disk removal is not known until you try to communicate with the disk. To detect such removals, the disks can be polled periodically (every 20 seconds) using the **fcinterop loop-monitor** command. This command enables loop polling for FL ports in a Cisco MDS 9000 Family switch. By default, the **fcinterop loop-monitor** command is disabled.



Caution

Changes to the loop monitoring feature should be made by an administrator or individual who is completely familiar with switch operations.

Configuring the Switch for Interoperability

Interoperability enables multiple vendor products come into contact with each other. Fibre Channel standards guide vendors towards common external Fibre Channel interfaces.

If all vendors followed the standards in the same manner, then interconnecting different products would become a trivial exercise. However, not all vendors follow the standards in the same way thus resulting in interoperability modes. This section briefly explains the basic concepts of these modes.

Each vendor has a regular mode and an equivalent interoperability mode, which specifically turns off advanced or proprietary features and provide the product with a more amiable standards compliant implementation.

[Table 31-2](#) lists the changes in switch behavior when you enable interoperability mode. These changes are specific to switches in the Cisco MDS 9000 Family while in interop mode.

Table 31-2 *Changes in Switch Behavior When Interoperability Is Enabled*

Switch Feature	Changes if Interoperability is Enabled
Domain IDs	Some vendors cannot use the full range of 239 domains within a fabric. Domain IDs are restricted to the range 97-127. This is to accommodate the McData nominal restriction to this same range. They can either be setup statically (the MDS will only accept one domain ID, if it does not get that domain ID it isolates itself from the fabric), or preferred. (If it does not get its requested domain ID, it accepts any assigned domain ID.)
Timers	All Fibre Channel timers must be the same on all switches as these values are exchanged by E ports when establishing an ISL. The timers are:
F_S_TOV	Verify that the Fabric Stability Time Out Value timers match exactly.
D_S_TOV	Verify that the Distributed Services Time Out Value timers match exactly.
E_D_TOV	Verify that the Error Detect Time Out Value timers match exactly.

Table 31-2 *Changes in Switch Behavior When Interoperability Is Enabled (continued)*

Switch Feature	Changes if Interoperability is Enabled
R_A_TOV	Verify that the Resource Allocation Time Out Value timers match exactly.
Trunking	Trunking is not supported between two different vendor switches. This feature may be disabled on a per port or per switch basis.
Default zone	The default zone behavior of permit (all nodes can see all other nodes) or deny (all nodes are isolated when not explicitly placed in a zone), may change.
Zoning attributes	<p>Zones may be limited to the pWWN and other proprietary zoning methods (physical port number), may be eliminated.</p> <p>Note Brocade uses the cfgsave command to save fabric-wide zoning configuration. This command doesn't have any effect on Cisco MDS 9000 Family switches if they are part of the same fabric. You must explicitly save the configuration on each switch in the Cisco MDS 9000 Family using the copy running start command.</p>
Zone propagation	<p>Some vendors do not pass the full zone configuration (zoneset) to other switches, only the active zoneset gets passed.</p> <p>Verify that the active zoneset or zone configuration has correctly propagated to the other switches in the fabric.</p>
VSAN	Interop mode only affects the specified VSAN.
TE ports and PortChannels	TE ports and Port-Channels cannot be used to connect MDS to non-MDS switches. Only E ports can be used to connect to non-MDS switches. TE ports and PortChannels can still be used to connect an MDS to other MDS switches even when in interop mode.
FSPF	The routing of frames within the fabric is not changed by the introduction of interop mode. The switch continues to use src-id, dst-id, and ox-id to load balance across multiple ISL links.
Domain reconfiguration disruptive	This is a switch-wide impacting event. Brocade and McData require the entire switch to be placed in offline mode and/or rebooted when changing Domain IDs.
Domain reconfiguration nondisruptive	This event is limited to the affected VSAN. Only Cisco MDS 9000 Family switches have this capability--only the domain manager process for the affected VSAN is restarted and not the entire switch.
Name server	Verify that all vendors have the correct values in their respective name server database.
IVR	Prior to Cisco MDS SAN-OS Release 1.3(4a), IVR-enabled VSANs can only be configured in no interop (default) mode or in interop mode 1. As of Cisco MDS SAN-OS Release 1.3(4a), IVR-enabled VSANs can be configured in no interop (default) mode or in any interop mode.

Configuring Interoperability

The **interop** mode in Cisco MDS 9000 Family switches can be enabled disruptively or nondisruptively. Brocade's **msplmgmtdeactivate** command must explicitly be run prior to connecting from a Brocade switch to either Cisco MDS 9000 Family switches or to McData switches. This command uses Brocade proprietary frames to exchange platform information, which Cisco MDS 9000 Family switches and McData switches do not understand. Rejecting these frames causes the common E ports to become isolated.

Using the show tech-support Command

The **show tech-support** command is useful when collecting a large amount of information about your switch for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem.

The **show tech-support** command displays the output of several **show** commands at once. The output from this command will vary depending on your configuration. Use the **show tech-support** command in EXEC mode to display general information about the switch when reporting a problem.

You can choose to have detailed information for each command or even specify the output for a particular interface, module or VSAN. Each command output is separated by line and the command precedes the output.



Note

Explicitly set the **terminal length** command to 0 (zero) to disable auto-scrolling and enable manually scrolling. Use the **show terminal** command to view the configured the terminal size. After obtaining the output of this command, remember to reset your terminal length as required



Tip

You can save the output of this command to a file by appending > filename to the **show tech-support** command. If you save this file, verify you have sufficient space to do so--each of these files may take about 1.8 MB. However, you can zip this file using the **gzip** filename command. Copy the zipped file to the required location using the **copy** command and unzip the file using the **gunzip** command

The default output of the **show tech-support** command includes the output of the following commands:

- **show version**
- **show environment**
- **show module**
- **show hardware**
- **show running-config**
- **show interface**
- **show accounting log**
- **show process**
- **show process log**
- **show processes log details**
- **show flash**

Each command is discussed in both the *Cisco MDS 9000 Family Configuration Guide* and the *Cisco MDS 9000 Family Command Reference*. Refer to the *Cisco MDS 9000 Family Troubleshooting Guide* to obtain debug processes, procedures, and examples.

Managing World Wide Names

Each port on a Cisco MDS 9000 Family switch is uniquely identified by its world wide names (WWNs), which include the switch MAC address and an identifier for each port. The principal switch selection and the allocation of domain IDs use the WWN to identify a specific port.

To add WWNs, perform the following steps.

-
- | | |
|---------------|--|
| Step 1 | From the Fabric Manager, choose FC > WWN Manager on the menu tree, or from the Device Manager, choose FC > WWN Manager . |
| | The Information pane of the Fabric Manager displays WWN information for multiple switches. The dialog box from the Device Manager displays WWN information for a single switch. |
| Step 2 | Configure the BaseMacAddress and MacAddressRange attributes for the WWN(s). |
| Step 3 | In the Fabric Manager Information pane, the information is updated. In the Device Manager dialog, click Apply to accept the changes; click Close to close the WWN Manager dialog without saving changes. |
-

Configuring Timers

To configure timers from the Fabric Manager, choose FC > Timers & Policies on the menu tree. The Information pane from the Fabric Manager displays timers for multiple switches.

To configure timers from the Device Manager, choose FC > Timers/Policies. The dialog box from the Device Manager displays timers for a single switch.

