CHAPTER 23

Advanced Features and Concepts

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

Configuring Time Out Values

The **fctimer** command modifies Fibre Channel protocol related timer values for the switch. You can only configure Fibre Channel time out values (TOVs) commands if all VSANs in a switch are suspended.

Note The F_S_TOV constant can not be configured.

You can use the **fctimer** 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.
- Resource allocation ‘TOV (R_A_TOV)—the valid range is from 5,000 to 10,000 milliseconds. The default is 10,000 milliseconds.

Caution These values can not be changed unless all VSANs in the switch are suspended.

If you issue the **fctimer** command without suspending all VSANs in a switch, you will get a warning message:

```
switch# fctimer D_S_TOV 6000
Warning: This configuration would impact whole fabric.
Since this configuration is not propagated to other switches.
Please configure the same value in all the switches
It is recommended that all vsans be suspended before executing this command
suspend all vsans first
could not update the value
switch#
```

Use the **show fctimer** command to display show the configured fctimer values (see Example 23-1).

Example 23-1 Displays Configured TOVs

```
switch# show fctimer
F_S_TOV : 5000 milliseconds
D_S_TOV : 5000 milliseconds
E_D_TOV : 2000 milliseconds
R_A_TOV : 10000 milliseconds
```

Note The F_S_TOV constant, though not configured, is displayed in the output of the **show fctimer** command.

Invoking fctrace

The fctrace feature allows you to:

- Trace the route followed by data traffic.
- Compute inter-switch (hop-to-hop) latency.

You can invoke fctrace by providing the FC ID, the N port, or the NL port WWN of the destination. The frames are routed normally as long as they are forwarded through TE ports.

Once the frame reaches the edge of the fabric (the F port or FL port connected to the end node with the given port WWN or the FC ID), the frame is looped back (swapping the source ID and the destination ID) to the originator.

If the destination cannot be reached the path discovery starts, which traces the path up to the point of failure.

Note The fctrace feature works only on TE Ports. Make sure that only TE ports exist in the path to the destination. In case there is an E Port in the path, the fctrace frame is dropped by that switch. Also, fctrace times out in the originator, and path discovery does not start.

To perform a fctrace operation, follow this step:

	Command	Purpose

Step 1	`switch# fctrace fcid 0xd70000 vsan 1`
	`Route present for : 0xd70000`
	`20:00:00:0b:46:00:02:82(0xfffcd5)`
	`Timestamp Invalid.`
	`20:00:00:05:30:00:18:db(0xfffcd7)`
	`Timestamp Invalid.`
	`20:00:00:05:30:00:18:db(0xfffcd7)`
		Invokes fctrace for the specified FC ID of the destination N port

	`switch# fctrace pwwn 21:00:00:e0:8b:06:d9:1d vsan 1 timeout 5`
	`Route present for : 21:00:00:e0:8b:06:d9:1d`
	`20:00:00:0b:46:00:02:82(0xfffcd5)`
	`Timestamp Invalid.`
	`20:00:00:05:30:00:18:db(0xfffcd7)`
	`Timestamp Invalid.`
	`20:00:00:05:30:00:18:db(0xfffcd7)`
		Invokes fctrace using the pWWN of the destination N port
		By default the period to wait before timing out is 5 seconds, The range is from one through 10 seconds.

Note You cannot use the fctrace feature in a locally configured VSAN interface (IPFC interface), but you can trace the route to a VSAN interface configured in other switches.

Invoking fcping

The fcping feature verifies reachability of a node by checking its end-to-end connectivity. You can invoke the fcping feature by providing the FC ID or the destination port WWN information.

To perform a fcping operation, follow this step:

	Command	Purpose

Step 1	`switch# fcping fcid 0xd70000 vsan 1`
	`28 bytes from 0xd70000 time = 730 usec`
	`28 bytes from 0xd70000 time = 165 usec`
	`28 bytes from 0xd70000 time = 262 usec`
	`28 bytes from 0xd70000 time = 219 usec`
	`28 bytes from 0xd70000 time = 228 usec`
	
	`5 frames sent, 5 frames received, 0 timeouts`
	`Round-trip min/avg/max = 165/270/730 usec`
		Performs a fcping operation for the specified pWWN or the FCID of the destination. By default, five frames are sent.

	`switch# fcping fcid 0xd70000 vsan 1 count 10`
	`28 bytes from 0xd70000 time = 730 usec`
	`28 bytes from 0xd70000 time = 165 usec`
	`28 bytes from 0xd70000 time = 262 usec`
	`28 bytes from 0xd70000 time = 219 usec`
	`28 bytes from 0xd70000 time = 228 usec`
	`28 bytes from 0xd70000 time = 230 usec`
	`28 bytes from 0xd70000 time = 230 usec`
	`28 bytes from 0xd70000 time = 225 usec`
	`28 bytes from 0xd70000 time = 229 usec`
	`28 bytes from 0xd70000 time = 183 usec`
	
	`10 frames sent, 10 frames received, 0 timeouts`
	`Round-trip min/avg/max = 165/270/730 usec`
		Sets the number of frames to be sent using the count option. The range is from 0 through 2147483647. A value of 0 will ping forever.

	`switch# fcping fcid 0xd500b4 vsan 1 timeout 10`
	`28 bytes from 0xd500b4 time = 1345 usec`
	`28 bytes from 0xd500b4 time = 417 usec`
	`28 bytes from 0xd500b4 time = 340 usec`
	`28 bytes from 0xd500b4 time = 451 usec`
	`28 bytes from 0xd500b4 time = 356 usec`
	
	`5 frames sent, 5 frames received, 0 timeouts`
	`Round-trip min/avg/max = 340/581/1345 usec`
		Sets the timeout value. The default period to wait is 5 seconds. The range is from 1 through 10 seconds.

Step 2	`switch# fcping fcid 0x010203 vsan 1`
	`No response from the N port.`
	
	`switch# fcping pwwn 21:00:00:20:37:6f:db:dd vsan 1`
	`28 bytes from 21:00:00:20:37:6f:db:dd time = 1454 usec`
	`28 bytes from 21:00:00:20:37:6f:db:dd time = 471 usec`
	`28 bytes from 21:00:00:20:37:6f:db:dd time = 372 usec`
	`28 bytes from 21:00:00:20:37:6f:db:dd time = 364 usec`
	`28 bytes from 21:00:00:20:37:6f:db:dd time = 1261 usec`
	
	`5 frames sent, 5 frames received, 0 timeouts`
	`Round-trip min/avg/max = 364/784/1454 usec`
		Issues a `No response from the N port` message even when the N port or NL port is active. This is due to resource exhaustion at the N port or NL port.
		
		Retry the command a few seconds later.

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.

Cisco's 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 Cisco's 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.

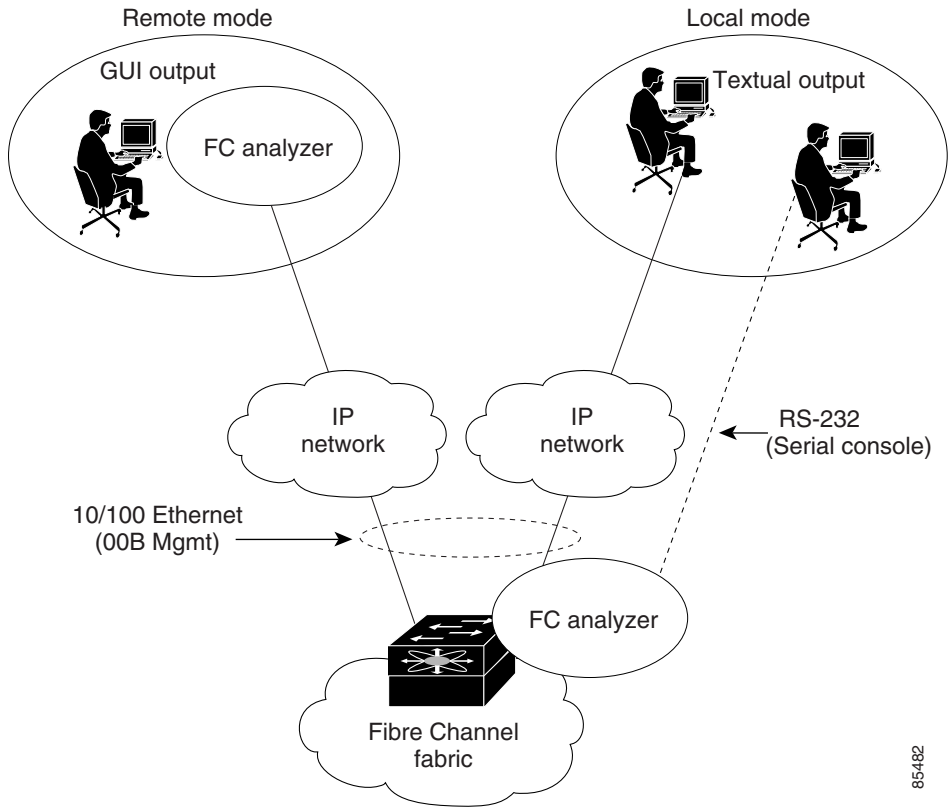
This section explains the following topics:

About the Cisco Fabric Analyzer

The Cisco Fabric Analyzer comprises two separate components (see Figure 23-1):

- 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 23-1 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.

See the "Capturing Frames Locally" section on page 23-7.

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.

See the "Sending Captures to Remote IP Addresses" section on page 23-9.

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 Ethereal's 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.

See the "Display Filters" section on page 23-10.

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.

Capturing Frames Locally

Launches the textual version on the analyzer directly on the console screen. The capture can also be saved on the local file system.

To capture frames locally, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
	Note The options within Step 2 may be performed in any order.	

	Command	Purpose

Step 2	`switch(config)# fcanalyzer local`
	`Capturing on eth2`
	`switch(config)#`
		Begins capturing the frames locally (supervisor module).

	`switch(config)# fcanalyzer local brief`
	`Capturing on eth2`
	`switch(config)#`
		Displays the protocol summary in a brief format.

	`switch(config)# fcanalyzer local display-filter SampleF` `Capturing on eth2`	Displays the filtered frames.

	`switch(config)# fcanalyzer local limit-frame-size 64`
	`Capturing on eth2`
	`switch(config)#`
		Limits the size of the frame capture to the first 64 bytes. The allowed range is 64 to 65536 bytes.

	`switch(config)# fcanalyzer local limit-captured-frames 10`
	`Capturing on eth2`
	`switch(config)#`
		Limits the number of frames captured to 10. The allowed range is 0 to 2147483647 frames and the default is 100 frames. Use 0 if you do not want to limit the number of captured frames.

	Note Press **Ctrl-c** to stop a capture. Otherwise, the capture stops automatically after capturing 100 frames. You can change this default using the **fcanalyzer local limit-captured-frames** ***number*** command.	

Step 3	`switch(config)# fcanalyzer local write SampleFile`
	`Capturing on eth2`
	`switch(config)#`
		Saves the captured frames to a specified file (SampleFile).

	Note The final filename that is the capture file will be called either SampleFile_00000_<dateandtime> or SampleFile_00001_<dateandtime>. For example, “SampleFile_00000_20021110223833” or “SampleFile_00001_20021110243833”. The maximum size of a file that can be written to is 10MB.	

Sending Captures to Remote IP Addresses

Caution You must use the eth2 interface to capture control traffic on a supervisor-module.

To capture frames remotely, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# fcanalyzer remote 10.21.0.3` `switch(config)#`	Configures the remote IP address (10.21.0.3) to which the captured frames will be sent.
Step 3	`switch(config)# fcanalyzer remote 10.21.0.3 active` `switch(config)#`	Enables active mode (passive is the default) with the remote host. Ethereal is assumed to be running when the capture is performed. The switch tries to connect forever unless a capture stop instruction is sent from Ethereal.
	`switch(config)# fcanalyzer remote 10.21.03 active 1` `switch(config)#`	Enables the active mode for a specified port. The valid port range is 1 to 65535.

To capture remote traffic, use one of the following options:

- To specify the capture interface in Ethereal as the remote device:

  ```
  rpcap://<ipaddress or switch hostname>/eth2
  ```

  For example:

  ```
  rpcap://cp-16/eth2
  rpcap://17.2.1.1/eth2
  ```

- The capture interface can be specified either in the capture dialog box or via the -i option at the command line when invoking Ethereal.

  ```
  ethereal -i rpcap://<ipaddress|hostname>[:<port>]/<interface>
  ```

  For example:

  ```
  ethereal -i rpcap://172.22.1.1/eth2.
  ```

  or

  ```
  ethereal -i rpcap://customer-switch.customer.com/eth2.
  ```

Clearing Configured fcanalyzer Information

Use the **clear fcanalyzer** command to clear the entire list of configured hosts. Note that the existing connections are not terminated.

Viewing Display Filters Information

Use the **show fcanalyzer** command to display the list of hosts configured for a remote capture. See Example 23-2.

Example 23-2 Displays Configured Hosts

```
switch# show fcanalyzer
PassiveClient = 10.21.0.3
PassiveClient = 10.21.0.3
ActiveClient = 10.21.0.3, DEFAULT
```

Note The DEFAULT in the ActiveClient line indicates that the default port is used.

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 only want to view ELP request frames. This feature only limits the captured view—it does not affect the captured or the saved frames. Procedures to specify, use, and save display filters are already document in the Ethereal web site (http://www.ethereal.com). Some examples of how you can use this feature are provided below:

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

  ```
  mdshdr.vsan == 2
  ```

- To view all SW_ILS frames, use this expression:

  ```
  fcswils
  ```

- To view class F frames, use this expression:

  ```
  mdshdr.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 1, use this expression:

  ```
  fcels.opcode == FLOGI && mdshdr.vsan == 2
  ```

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

  ```
  dNS
  ```

Defining Display Filters

Display filters limit the frames that can be displayed, but not what is captured (similar to any view command). The filters to be displayed can be defined in multiple ways in the GUI application:

- Auto-definition
- Manual definition
- Assisted manual definition
- Only manual definition in local capture
- No assists

Regardless of the definition, each filter must be saved and identified with a name.

Note This GUI-assisted feature is part of Ethereal and you can obtain more information from http://www.ethereal.com.

Capture Filters

You can limit what frames are captures by using the capture filters feature in a remote capture. This feature limits the frames that are captured and sent from the remote switch to the host. For example, you can capture only class F frames. Capture filters is useful in restricting the amount of bandwidth consumed by the remote capture.

Unlike display filters, capture filters restricts a capture to the specified frames. No other frames will be visible until you specify a completely new capture.

The syntax for capture filter is different from the syntax for display filters. Capture filters use the Berkeley Packet Filter (BPF) library that is used in conjunction with the libpcap freeware. The list of all valid Fibre Channel capture filter fields are provided later in this section.

Procedures to configure capture filters are already document in the Ethereal web site (http://www.ethereal.com). Some examples of how you can use this feature are provided below:

- To capture frames only on a specified VSAN, use this expression:

  ```
  vsan = 1
  ```

- To capture only class F frames, use this expression:

  ```
  class_f
  ```

- To capture only class Fibre Channel ELS frames, use this expression:

  ```
  els
  ```

- To capture only name server frames, use this expression:

  ```
  dns
  ```

- To capture only SCSI command frames, use this expression:

  ```
  fcp_cmd
  ```

Note This feature is part of libpcap and you can obtain more information from http://www.tcpdump.org.

Permitted Capture Filters

```
o vsan
o src_port_idx
o dst_port_idx
o sof
o r_ctl
o d_id
o s_id
o type
o seq_id
o seq_cnt
o ox_id
o rx_id
o els
o swils
o fcp_cmd   (FCP Command frames only)
o fcp_data (FCP data frames only)
o fcp_rsp   (FCP response frames only)
o class_f
o bad_fc
o els_cmd
o swils_cmd
o fcp_lun
o fcp_task_mgmt
o fcp_scsi_cmd
o fcp_status
o gs_type      (Generic Services type)
o gs_subtype   (Generic Services subtype)
o gs_cmd
o gs_reason
o gs_reason_expl
o dns   (name server)
o udns (unzoned name server)
o fcs   (fabric configuration server)
o zs    (zone server)
o fc    (use as fc[x:y] where x is offset and y is length to compare)
o els   (use as els[x:y] similar to fc)
o swils (use as swils[x:y] similar to fc)
o fcp   (use as fcp[x:y] similar to fc)
o fcct (use as fcct[x:y] similar to fc)
```

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's 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 (see Table 23-1).

Table 23-1 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 are only performed as required. They should not be changed on a daily basis. These changes should be made by an administrator or individual who is completely familiar with switch operations.

Configuring a Secondary MAC Address

To register the port ID objects, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.

Step 2	`switch(config)# wwnm secondary-mac 00:99:55:77:55:55 range 64`
	`This command CANNOT be undone.`
	`Please enter the BASE MAC ADDRESS again: 00:99:55:77:55:55`
	`Please enter the mac address RANGE again: 64`
	`From now on WWN allocation would be based on new MACs.`
	`Are you sure? (yes/no) no`
	`You entered: no. Secondary MAC NOT programmed`
	`switch(config)#`
		Configures the secondary MAC address. This command cannot be undone.

Displaying WWN Information

Use the **show wwn** commands to display the status of the WWN configuration. See Examples 23-3 to 23-6.

Example 23-3 Displays the Status of All WWNs

```
switch# show wwn status
         Type 1 WWNs: Configured:     64 Available:     48 (75%) Resvd.: 16
    Types 2 & 5 WWNs: Configured: 524288 Available: 450560 (85%) Resvd.: 73728
NKAU & NKCR WWN Blks: Configured:   1760 Available:   1760 (100%)
        Alarm Status:      Type1:   NONE Types 2&5:   NONE
```

Example 23-4 Displays Specified Block ID Information:

```
switch# show wwn status block-id 51
WWNs in this block: 21:00:ac:16:5e:52:00:03 to 21:ff:ac:16:5e:52:00:03
Num. of WWNs:: Configured: 256 Allocated:    0 Available: 256
Block Allocation Status: FREE
```

Example 23-5 Displays the WWN for a Specific Switch

```
switch# show wwn switch
Switch WWN is 20:00:ac:16:5e:52:00:00
```

Example 23-6 Displays the WWN for a Specified VSAN

```
switch# show wwn vsan 1
VSAN WWN of VSAN# 1 is 20:01:ac:16:5e:52:00:01
```

Allocating Flat FC IDs

Based on Fibre Channel standards, one area is allocated to the N port attached to an F port in any switch. To save the number of FC IDs used, Cisco MDS 9000 Family switches provide a feature where each N ports can be assigned a single FC ID instead.

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

To allocate flat FC IDs, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# fcinterop fcid-allocation none` `switch(config)#`	Allocates one area to the N port attached to an F port.
	`switch(config)# fcinterop fcid-allocation flat` `switch(config)#`	Allocates a single FC ID to the N port. This option is generally used to conserve FC ID usage.
	`switch(config)# fcinterop fcid-allocation auto` `switch(config)#`	Intelligently assigns flat FC ID to N ports which can interoperate in **flat** mode, otherwise assigns full area to all other ports. This is the default.

Caution Changes to FC IDs are only performed as required. They should not be changed on a daily basis. These changes 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.

To enable the loop monitoring feature, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# fcinterop loop-monitor`	Enables the loop monitoring feature.
	`switch(config)# no fcinterop loop-monitor`	Disables (default) the loop monitoring feature and reverts the switch to the factory defaults.

Caution Changes to the loop monitoring feature are only performed as required. They should not be changed on a daily basis. These changes should be made by an administrator or individual who is completely familiar with switch operations.

Configuring the Switch for Interoperability

Interoperability enables multiple vendors' 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 aimiable standards compliant implementation.

Table 23-2 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 23-2 Changes in switch Behavior when Interoperability Is Enable

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 McData's nominal restriction to this same range. They can either be setup statically (the MDS will only accept one domain ID, if it doesn't get that domain ID it isolates itself from the fabric), or preferred. (If it doesn't 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.
R_A_TOV	Verify that the Resource Allocation Time Out Value timers match exactly.
Trunking	Trunking is not supported between two different vendor's 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	Zones may be limited to the pWWN and other proprietary zoning methods (physical port number), may be eliminated.
Zone propagation	Some vendors do not pass the full zone configuration (**zoneset**) to other switches, only the active zoneset gets passed. Verify that the active zoneset or zone configuration has correctly propagated to the other switches in the fabric.
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.

Table 23-2 Changes in switch Behavior when Interoperability Is Enable (continued)

Switch Feature	Changes if Interoperability Is Enabled
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 loadbalance 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.

Configuring Interoperability

The **interop** mode in Cisco MDS 9000 Family switches can be enabled disruptively or nondisruptively. The interoperability procedure is different in Cisco MDS 9500 Series and 9200 Series switches.

Note Brocade's `msplmgmtdeactivate` command must explicitly be run prior to connect 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 or McData switches do not understand. Rejecting these frames, causes the common E ports to become isolated.

Cisco MDS 9500 Series Switches

To configure interoperability in a Cisco MDS 9500 Series switch, follow these steps:

Step 1 Place the VSAN of the E ports (s) that connect to the OEM switch in interoperability mode.

```
switch# config t
switch(config)# vsan database
switch (config-vsan-db)# vsan 1 interop
```

Step 2 Assign a domain ID in the range of 97 (0x61) through 127 (0x7F).

Note This is an limitation imposed by the McData switches.

```
switch# config t
switch(config)# fcdomain domain 100 preferred vsan 1
```

In Cisco MDS 9000 switches, the default is to request an ID from the principle switch. If the **preferred** option is used, Cisco MDS 9000 switches request a specific ID, but still join the fabric if the principle switch assigns a different ID. If the **static** option is used, the Cisco MDS 9000 switches does not join the fabric unless the principle switch agrees, and assigns the requested ID.

Note When changing the Domain ID, the FC IDs assigned to N ports will also change.

Step 3 Change the Fibre Channel timers (if they have been changed from the system defaults).

Note The MDS 9000, Brocade, and McData FC Error Detect (ED_TOV) and Resource Allocation (RA_TOV) timers default to the same values. They can be changed if needed. The RA_TOV default is 10 seconds, and the ED_TOV default is 2 seconds. Per the FC-SW2 standard, these values must be the same on each switch within the fabric.

```
switch# config t
switch(config)# fctimer e_d_tov ?
  <1000-100000>  E_D_TOV in milliseconds(1000-100000)
switch(config)# fctimer r_a_tov ?
  <5000-100000>  R_A_TOV in milliseconds(5000-100000)
```

Step 4 When making changes to the domain, you may or may not need to restart the MDS domain manager function for the altered VSAN.

a. Force a fabric reconfiguration with the **disruptive** option.

```
switch(config)# fcdomain restart disruptive vsan 1
```

or

b. Don't force a fabric reconfiguration

```
switch(config)# fcdomain restart vsan 1
```

Cisco MDS 9200 Series Switches

To configure interoperability in a Cisco MDS 9200 Series switch, follow these steps:

Step 1 Place the VSAN of the E ports (s) that connect to the OEM switch in interoperability mode.

```
switch# config t
switch(config)# vsan database
switch(config-vsan-db)# vsan 1 interop
```

Step 2 Assign a domain ID in the range of 97 (0x61) through 127 (0x7F).

Note This is an limitation imposed by the McData switches.

```
switch# config t
switch(config)# fcdomain domain 100 preferred vsan 1
```

In Cisco MDS 9000 switches, the default is to request an ID from the principle switch. If the **preferred** option is used, Cisco MDS 9000 switches request a specific ID, but still join the fabric if the principle switch assigns a different ID. If the **static** option is used, the Cisco MDS 9000 switches does not join the fabric unless the principle switch agrees, and assigns the requested ID.

Note When changing the Domain ID, the FC IDs assigned to N ports will also change.

Step 3 Change the Fibre Channel timers (if they have been changed from the system defaults).

Note The MDS 9000, Brocade, and McData FC Error Detect (ED_TOV) and Resource Allocation (RA_TOV) timers default to the same values. They can be changed if needed. The RA_TOV default is 10 seconds, and the ED_TOV default is 2 seconds. Per the FC-SW2 standard, these values must be the same on each switch within the fabric.

```
switch# config t
switch(config)# fctimer e_d_tov ?
  <1000-100000>  E_D_TOV in milliseconds(1000-100000)
switch(config)# fctimer r_a_tov ?
  <5000-100000>  R_A_TOV in milliseconds(5000-100000)
```

Step 4 When making changes to the domain, you may or may not need to restart the MDS domain manager function for the altered VSAN.

a. Force a fabric reconfiguration with the **disruptive** option.

```
switch(config)# fcdomain restart disruptive vsan 1
```

or

b. Don't force a fabric reconfiguration

```
switch(config)# fcdomain restart vsan 1
```

Verifying Interoperating Status

This section highlights the commands used to verify if the fabric is up and running in interoperability mode.

Cisco MDS 9500 Series Switches

To verify the resulting status of issuing the interoperability command in a Cisco MDS 9500 Series switch, follow these steps:

Step 1 Use the **show version** command to verify the version.

```
switch# show ver
Copyright (c) 2001-2005
Cisco Systems, Inc.
Software
  kickstart: version 1.0(2a) [gdb]
  System:    version 1.0(2a) [gdb]
Hardware
  RAM 1932864 kB
  bootflash: 503808 blocks (block size 512b)
  slot0:          0 blocks (block size 512b)
  Compile Time: 10/26/2002 2:00:00
```

Step 2 Use the **show interface brief** command to verify if the interface states are as required by your configuration

```
switch# show int brief
Interface  Vsan   Admin  Admin   Status          Oper  Oper   Port-channel
```

```
                    Mode    Trunk                    Mode   Speed
                            Mode                             (Gbps)
------------------------------------------------------------------------------
fc2/1       1       auto    on       up              E      2       --
fc2/2       1       auto    on       up              E      2       --
fc2/3       1       auto    on       fcotAbsent      --     --      --
fc2/4       1       auto    on       down            --     --      --
fc2/5       1       auto    on       down            --     --      --
fc2/6       1       auto    on       down            --     --      --
fc2/7       1       auto    on       up              E      1       --
fc2/8       1       auto    on       fcotAbsent      --     --      --
fc2/9       1       auto    on       down            --     --      --
fc2/10      1       auto    on       down            --     --      --
```

Step 3 Use the **show run** command to verify if you are running the desired configuration.

```
switch# show run
Building Configuration...

 interface fc2/1
no shutdown

 interface fc2/2
no shutdown

 interface fc2/3
 interface fc2/4
 interface fc2/5
 interface fc2/6
 interface fc2/7
no shutdown

 interface fc2/8
 interface fc2/9
 interface fc2/10

<snip>

interface fc2/32

 interface mgmt0
ip address 6.1.1.96 255.255.255.0
switchport encap default
no shutdown

vsan database
vsan 1 interop

boot system bootflash:/m9500-system-253e.bin sup-1
boot kickstart bootflash:/m9500-kickstart-253e.bin sup-1
boot system bootflash:/m9500-system-253e.bin sup-2
boot kickstart bootflash:/m9500-kickstart-253e.bin sup-2
callhome

fcdomain domain 100 preferred vsan 1

ip route 6.1.1.0 255.255.255.0 6.1.1.1
ip routing
line console
  databits 5
  speed 110
logging linecard
ssh key rsa 512 force
ssh server enable
```

```
switchname MDS9509
username admin password 5 $1$Li8/fBYX$SNc72.xt4nTXpSnR9OUFB/ role network-admin
```

Step 4 Use the **show vsan** command to verify if the interoperability mode is active.

```
switch# show vsan 1
vsan 1 information
         name:VSAN0001 stalactites
         interoperability mode:yes <-------------------- verify mode
         loadbalancing:src-id/dst-id/oxid
         operational state:up
```

Step 5 Use the **show fcdomain vsan** command to verify the domain ID.

```
switch# show fcdomain vsan 1
The local switch is a Subordinated Switch.

Local switch run time information:
        State: Stable
        Local switch WWN:    20:01:00:05:30:00:51:1f
        Running fabric name: 10:00:00:60:69:22:32:91
        Running priority: 128
        Current domain ID: 0x64(100) <---------------verify domain id

Local switch configuration information:
        State: Enabled
        Auto-reconfiguration: Disabled
        Contiguous-allocation: Disabled
        Configured fabric name: 41:6e:64:69:61:6d:6f:21
        Configured priority: 128
        Configured domain ID: 0x64(100) (preferred)

Principal switch run time information:
        Running priority: 2

Interface               Role          RCF-reject
----------------    -------------    ------------
fc2/1               Downstream       Disabled
fc2/2               Downstream       Disabled
fc2/7               Upstream         Disabled
----------------    -------------    ------------
```

Step 6 Use the **show fcdomain domain-list vsan** command to verify the local principal switch status.

```
switch# show fcdomain domain-list vsan 1

Number of domains: 5
Domain ID              WWN
---------    -----------------------
 0x61(97)    10:00:00:60:69:50:0c:fe
 0x62(98)    20:01:00:05:30:00:47:9f
 0x63(99)    10:00:00:60:69:c0:0c:1d
0x64(100)    20:01:00:05:30:00:51:1f [Local]
0x65(101)    10:00:00:60:69:22:32:91 [Principal]
---------    -----------------------
```

Step 7 Use the **show fspf internal route vsan** command to verify the next hop and destination for the switch.

```
switch# show fspf internal route vsan 1

FSPF Unicast Routes
---------------------------
 VSAN Number  Dest Domain   Route Cost    Next hops
---------------------------------------------
           1     0x61(97)          500      fc2/2
```

```
1     0x62(98)         1000      fc2/1
                                 fc2/2
1     0x63(99)          500      fc2/1
1    0x65(101)         1000      fc2/7
```

Step 8 Use the **show fcns data vsan** command to verify the name server information.

```
switch# show fcns data vsan 1
VSAN 1:
--------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------
0x610400    N     10:00:00:00:c9:24:3d:90 (Emulex)     scsi-fcp
0x6105dc    NL    21:00:00:20:37:28:31:6d (Seagate)    scsi-fcp
0x6105e0    NL    21:00:00:20:37:28:24:7b (Seagate)    scsi-fcp
0x6105e1    NL    21:00:00:20:37:28:22:ea (Seagate)    scsi-fcp
0x6105e2    NL    21:00:00:20:37:28:2e:65 (Seagate)    scsi-fcp
0x6105e4    NL    21:00:00:20:37:28:26:0d (Seagate)    scsi-fcp
0x630400    N     10:00:00:00:c9:24:3f:75 (Emulex)     scsi-fcp
0x630500    N     50:06:01:60:88:02:90:cb              scsi-fcp
0x6514e2    NL    21:00:00:20:37:a7:ca:b7 (Seagate)    scsi-fcp
0x6514e4    NL    21:00:00:20:37:a7:c7:e0 (Seagate)    scsi-fcp
0x6514e8    NL    21:00:00:20:37:a7:c7:df (Seagate)    scsi-fcp
0x651500    N     10:00:00:e0:69:f0:43:9f (JNI)

Total number of entries = 12
```

Note The MDS Name Server shows both local and remote entries, and does not timeout the entries.

Cisco MDS 9200 Series Switches

To verify the resulting status of issuing the interoperability command in a Cisco MDS 9200 Series switch, follow these steps:

Step 1 Use the **show version** command to verify the version.

```
switch# show ver
Copyright (c) 2001-2005
Cisco Systems, Inc.
Software
  kickstart: version 1.0(2a) [gdb]
  System:    version 1.0(2a) [gdb]
Hardware
  RAM 963116 kB
  bootflash: 503808 blocks (block size 512b)
  slot0:          0 blocks (block size 512b)
  Compile Time: 10/26/2002 2:00:00
```

Step 2 Use the **show interface brief** command to verify if the interface states are as required by your configuration

```
switch# show int brief
--------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          Oper  Oper   Port-channel
                  Mode   Trunk                   Mode  Speed
                         Mode                          (Gbps)
--------------------------------------------------------------------
```

```
fc1/1      1      auto   on      up               E     2      --
fc1/2      1      auto   on      fcotAbsent       --    --     --
fc1/3      1      auto   on      up               E     2      --
fc1/4      1      auto   on      down             --    --     --
fc1/5      1      auto   on      down             --    --     --
fc1/6      1      auto   on      up               E     1      --
fc1/7      1      auto   on      fcotAbsent       --    --     --
fc1/8      1      auto   on      fcotAbsent       --    --     --
fc1/9      1      auto   on      down             --    --     --
```

Step 3 Use the **show run** command to verify if you are running the desired configuration.

```
switch# show run
Building Configuration...
 interface fc1/1
no shutdown
 interface fc1/2
 interface fc1/3
switchport speed 2000
no shutdown
 interface fc1/4
 interface fc1/5
 interface fc1/6
switchport speed 1000
no shutdown
 interface fc1/7
 interface fc1/8
 interface fc1/9
...
 interface mgmt0
ip address 6.1.1.95 255.255.255.0
no shutdown
vsan database
vsan 1 interop
boot system bootflash:/m9200-system-253e.bin
boot kickstart bootflash:/m9200-kickstart-253e.bin
callhome
fcdomain domain 98 preferred vsan 1
line console
  databits 5
  speed 110
logging linecard
switchname MDS9216
username admin password 5 MF7UQdWLEqUFE role network-admin
```

Step 4 Use the **show vsan** command to verify if the interoperability mode is active.

```
switch# show vsan 1
vsan 1 information
         name:VSAN0001 state:active
         interoperability mode:yes <---------------------- verify interoperability
         loadbalancing:src-id/dst-id/oxid
         operational state:up
```

Step 5 Use the **show fcdomain vsan** command to verify the domain ID.

```
switch# show fcdomain vsan 1
The local switch is a Subordinated Switch.

Local switch run time information:
        State: Stable
        Local switch WWN:    20:01:00:05:30:00:47:9f
        Running fabric name: 10:00:00:60:69:22:32:91
        Running priority: 128
        Current domain ID: 0x62(98) <-----------------------verify domain ID
```

```
Local switch configuration information:
        State: Enabled
        Auto-reconfiguration: Disabled
        Contiguous-allocation: Disabled
        Configured fabric name: 41:6e:64:69:61:6d:6f:21
        Configured priority: 128
        Configured domain ID: 0x62(98) (preferred)
Principal switch run time information:
        Running priority: 2
Interface               Role          RCF-reject
----------------    -------------    ------------
fc1/1               Upstream         Disabled
fc1/3               Non-principal    Disabled
fc1/6               Non-principal    Disabled
----------------    -------------    ------------
```

Step 6 Use the **show fcdomain domain-list vsan** command to verify the local principal switch status.

```
switch# show fcdomain domain-list vsan 1
Number of domains: 5
Domain ID              WWN
---------    -----------------------
 0x61(97)    10:00:00:60:69:50:0c:fe
 0x62(98)    20:01:00:05:30:00:47:9f [Local]
 0x63(99)    10:00:00:60:69:c0:0c:1d
0x64(100)    20:01:00:05:30:00:51:1f
0x65(101)    10:00:00:60:69:22:32:91 [Principal]
---------    -----------------------
```

Step 7 Use the **show fspf internal route vsan** command to verify the next hop and destination for the switch.

```
switch# show fspf internal route vsan 1
FSPF Unicast Routes
---------------------------
 VSAN Number  Dest Domain   Route Cost    Next hops
-----------------------------------------------
           1    0x61(97)           500        fc1/1
           1    0x63(99)           500        fc1/3
           1    0x64(100)         1000        fc1/1
                                             fc1/3
           1    0x65(101)         1000        fc1/6
```

Step 8 Use the **show fcns data vsan** command to verify the name server information.

```
switch# show fcns data vsan 1
VSAN 1:
--------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)  FC4-TYPE:FEATURE
--------------------------------------------------------------------
0x610400    N     10:00:00:00:c9:24:3d:90 (Emulex)     scsi-fcp
0x6105dc    NL    21:00:00:20:37:28:31:6d (Seagate)    scsi-fcp
0x6105e0    NL    21:00:00:20:37:28:24:7b (Seagate)    scsi-fcp
0x6105e1    NL    21:00:00:20:37:28:22:ea (Seagate)    scsi-fcp
0x6105e2    NL    21:00:00:20:37:28:2e:65 (Seagate)    scsi-fcp
0x6105e4    NL    21:00:00:20:37:28:26:0d (Seagate)    scsi-fcp
0x630400    N     10:00:00:00:c9:24:3f:75 (Emulex)     scsi-fcp
0x630500    N     50:06:01:60:88:02:90:cb              scsi-fcp
0x6514e2    NL    21:00:00:20:37:a7:ca:b7 (Seagate)    scsi-fcp
0x6514e4    NL    21:00:00:20:37:a7:c7:e0 (Seagate)    scsi-fcp
0x6514e8    NL    21:00:00:20:37:a7:c7:df (Seagate)    scsi-fcp
0x651500    N     10:00:00:e0:69:f0:43:9f (JNI)
Total number of entries = 12
```