CHAPTER 29

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 FC Timers

You can modify Fibre Channel protocol related timer values for the switch by configuring 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 Across All VSANs

You can modify Fibre Channel protocol related timer values for the switch using the **fctimer** command.

To configure FC timers across all VSANs, follow these steps:

	Command	Purpose

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

Step 2	`switch(config)# fctimer R_A_TOV 6000`	Configures the R_A_TOV value for all VSANs to be 6000 ms. This type of configuration is not permitted unless all VSANs are suspended.

Caution The D_S_TOV, E_D_TOV, and R_A_ TOV values cannot be globally changed unless all VSANs in the switch are suspended.

Note If a VSAN is not specified when you change the timer value, the changed value is applied to all VSANs in the switch.

Configuring Timers Per-VSAN

You can also issue the fctimer 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 that 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 Cisco MDS SAN-OS Release 1.2 or 1.1 after the timer is configured for a VSAN, an error message is issued to warn against strict incompatibilities. Refer to the *Cisco MDS 9000 Family Troubleshooting Guide*.

To configure per-VSAN FC timers, follow these steps:

	Command	Purpose

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

Step 2	`switch(config#)#` **`fctimer D_S_TOV 6000 vsan 2`**
	`Warning: The vsan will be temporarily suspended when updating the timer value This configuration would impact whole fabric. Do you want to continue? (y/n)` **`y`**
	`Since this configuration is not propagated to other switches, please configure the same value in all the switches`
		Configures the D_S_TOV value to be 6000 ms for VSAN 2. Suspends the VSAN temporarily. You have the option to end this command, if required.

Displaying Configured FC Timer Values

Use the **show fctimer** command to display the configured FC timer values (see Examples 29-1 and 29-2).

Example 29-1 Displays Configured Global TOVs

```
switch# show fctimer
F_S_TOV   D_S_TOV   E_D_TOV   R_A_TOV
----------------------------------------
5000 ms   5000 ms   2000 ms   10000 ms
```

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

Example 29-2 Displays Configured TOVs for a Specified VSAN

```
switch# show fctimer vsan 10
vsan no.  F_S_TOV   D_S_TOV   E_D_TOV   R_A_TOV
-------------------------------------------------
10        5000 ms   5000 ms   3000 ms   10000 ms
```

Invoking the fctrace Feature

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.

Tip 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.

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.

Invoking the fcping Feature

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 these steps:

	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`
		Invokes fcping for the specified pWWN or the FC ID 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 pings 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.

Verifying Switch Connectivity

You can also use the **fcping fcid** command to verify connectivity to a destination switch.

Note The FC ID variable used in this procedure is the domain controller address; it is not a duplication of the domain ID.

To verify connectivity to a destination switch, follow these steps:

	Command	Purpose
Step 1	switch# **show fcdomain domain-list vsan 200** Number of domains: 7 Domain ID WWN --------- ----------------------- 0x01(1) 20:c8:00:05:30:00:59:df [Principal] 0x02(2) 20:c8:00:0b:5f:d5:9f:c1 0x6f(111) 20:c8:00:05:30:00:60:df **0xda**(218) 20:c8:00:05:30:00:87:9f [Local] 0x06(6) 20:c8:00:0b:46:79:f2:41 0x04(4) 20:c8:00:05:30:00:86:5f 0x6a(106) 20:c8:00:05:30:00:f8:e3	Displays the destination switch's domain ID. To obtain the domain controller address, concatenate the domain ID with FFFC. For example, if the domain ID is 0xda(218), the concatenated ID is 0xfffcda.
Step 2	switch# **fcping fcid 0xFFFCDA vsan 200** 28 bytes from 0xFFFCDA time = 298 usec 28 bytes from 0xFFFCDA time = 260 usec 28 bytes from 0xFFFCDA time = 298 usec 28 bytes from 0xFFFCDA time = 294 usec 28 bytes from 0xFFFCDA time = 292 usec 5 frames sent, 5 frames received, 0 timeouts Round-trip min/avg/max = 260/288/298 usec	Verifies reachability of the destination switch by checking its end-to-end connectivity.

Configuring a Fabric Analyzer

Fibre Channel protocol analyzers capture, decode, and analyze frames and ordered sets on a link. 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 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—See http://www.tcpdump.org.
- Ethereal—See 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:

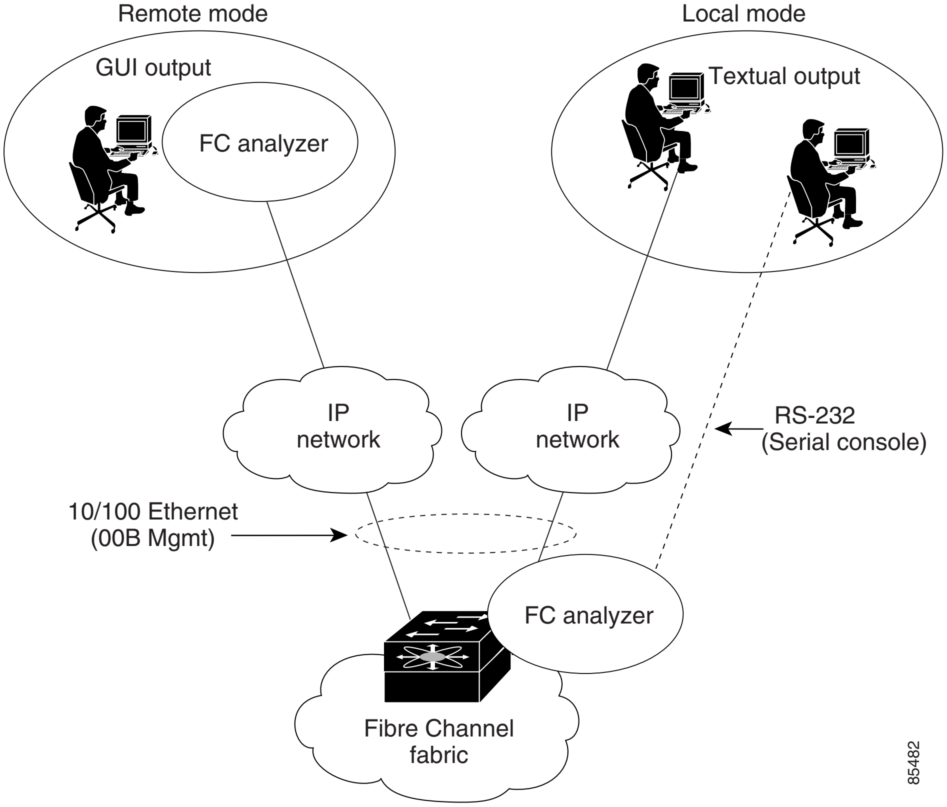
- About the Cisco Fabric Analyzer, page 29-7
- Configuring the Cisco Fabric Analyzer, page 29-9
- Clearing Configured fcanalyzer Information, page 29-11
- Displaying Configured Hosts, page 29-12
- Displaying Captured Frames, page 29-12

About the Cisco Fabric Analyzer

The Cisco Fabric Analyzer comprises of two separate components (see Figure 29-1):

- 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
- 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 29-1 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 Family 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 Family switch, it is protected by the roles-based policy that limits access in each switch.

See the "Capturing Frames Locally" section on page 29-9.

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 endpoints, 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 an unauthorized machine in the network from snooping on the control traffic in the network.

RPCAP supports two setup connection modes based on firewall 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 29-11.

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. The Ethereal GUI front-end supports a rich interface such as a colorized display, graphical assists in defining filters, and specific frame searches. These features are documented on Ethereal's website.

While remote capture through 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 "Displaying Captured Frames" section on page 29-12.

Configuring the Cisco Fabric Analyzer

You can configure the Cisco Fabric Analyzer to perform one of two captures.

- Local capture—The command setting to enable a local capture cannot be saved to persistent storage or synchronized to standby. Launches the textual version on the fabric analyzer directly on the console screen. The capture can also be saved on the local file system.
- Remote capture—The command setting to enable a remote capture can be saved to persistent storage. 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

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.

	Command	Purpose

Step 3	`switch(config)# fcanalyzer local write volatile:sample`
	`Capturing on eth2`
	`switch(config)#`
		Saves the captured frames to a specified file (sample) in the volatile: directory.
		Note Optionally, you can save the specified file to the slot0: directory.

Note The final filename that is the capture file is 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 10 MB.

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 are sent.

	`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 10.21.0.3 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:

- The capture interface can be specified 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 by using 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
  ```

Note For example, in a Windows 2000 setup, click **Start** on your desktop and select **Run**. In the resulting Run window, type the required command line option in the Open field.

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.

Displaying Configured Hosts

Use the **show fcanalyzer** command to display the list of hosts configured for a remote capture. See Example 29-3.

Example 29-3 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.

Displaying Captured Frames

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 documented in the Ethereal website (http://www.ethereal.com). Some examples of how you can use this feature are as follows:

- 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 == HLO || 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.

Displaying Filters Examples

Some examples of using display filters with the Fabric Analyzer local are provided in this section. The **brief** option is used in all examples to restrict the size of the output. See Example 29-4.

Example 29-4 Displays Only Fabric Login Server Traffic on VSAN 1

```
switch(config)# fcanalyzer local brief display-filter
mdshdr.vsan==0x01)&&((fc.d_id==\”ff.ff.fe\”\|\|fc.s_id==\"ff.ff.fe\"))
Capturing on eth2
8.904145   00.00.00 -> ff.ff.fe   FC ELS 1    0x28f8 0xffff  0x3 ->  0xf FLOGI
8.918164   ff.ff.fe -> 79.03.00   FC ELS 1    0x28f8 0x12c6 0xff ->  0x0 ACC (FLOGI)
```

You can trace all frames to and from a particular N port device. For example, to observe RSCNs from the Fabric Controller and registration and/or query requests to the name server. See Example 29-5.

Note The filter requires prior knowledge of the FC ID that is assigned to the N port. Issue the **show flogi database interface** command before running fcanalyzer to obtain the FC ID. In this example, the N port FC ID is 79.03.00.

Example 29-5 Displays All Traffic for a Particular N Port on VSAN 1

```
switch(config)# fcanalyzer local brief
display-filter(mdshdr.vsan==0x01)&&((fc.d_id==\”79.03.00\”\|\|fc.s_id==\"79.03.00\"))
Capturing on eth2
8.699162   ff.ff.fe -> 79.03.00   FC ELS 1    0x35b8 0x148e 0xff ->  0x0 ACC (FLOGI)
8.699397   79.03.00 -> ff.ff.fc   FC ELS 1    0x35d0 0xffff  0x3 ->  0xf PLOGI
8.699538   ff.ff.fc -> 79.03.00   FC ELS 1    0x35d0 0x148f 0xff ->  0x0 ACC (PLOGI)
8.699406   79.03.00 -> ff.ff.fd   FC ELS 1    0x35e8 0xffff  0x3 ->  0xf SCR
8.700179   79.03.00 -> ff.ff.fc   dNS    1    0x3600 0xffff  0x3 ->  0xf GNN_FT
8.702446   ff.ff.fd -> 79.03.00   FC ELS 1    0x35e8 0x1490 0xff ->  0x0 ACC (SCR)
8.704210   ff.ff.fc -> 79.03.00   dNS    1    0x3600 0x1491 0xff ->  0x0 ACC (GNN_FT)
8.704383   79.03.00 -> ff.ff.fc   dNS    1    0x3618 0xffff  0x3 ->  0xf GPN_ID
8.707857   ff.ff.fc -> 79.03.00   dNS    1    0x3618 0x1496 0xff ->  0x0 ACC (GPN_ID)
```

The VSAN ID is specified in hex. See Example 29-6.

Example 29-6 Displays All Traffic for a Specified VSAN

```
switch(config)# fcanalyzer local brief display-filter mdshdr.vsan==0x03e7
Capturing on eth2
12.762577   ff.ff.fd -> ff.ff.fd   SW_ILS 999   0xb2c 0xffff  0x1 ->  0xf HLO
12.762639   ff.ff.fd -> ff.ff.fd   FC     999   0xb2c  0xd32 0xff ->  0x0 Link Ctl, ACK1
13.509979   ff.ff.fd -> ff.ff.fd   SW_ILS 999   0xd33 0xffff 0xff ->  0x0 HLO
13.510918   ff.ff.fd -> ff.ff.fd   FC     999   0xd33  0xb2d  0x1 ->  0xf Link Ctl, ACK1
14.502391   ff.fc.64 -> ff.fc.70   SW_ILS 999   0xd34 0xffff 0xff ->  0x0 SW_RSCN
14.502545   ff.ff.fd -> 64.01.01   FC ELS 999   0xd35 0xffff 0xff ->  0x0 RSCN
14.502804   64.01.01 -> ff.ff.fd   FC ELS 999   0xd35  0x215  0x0 ->  0xf ACC (RSCN)
14.503387   ff.fc.70 -> ff.fc.64   FC     999   0xd34  0xb2e  0x1 ->  0xf Link Ctl, ACK1
14.503976   ff.fc.70 -> ff.fc.64   SW_ILS 999   0xd34  0xb2e  0x1 ->  0xf SW_ACC (SW_RSCN)
14.504025   ff.fc.64 -> ff.fc.70   FC     999   0xd34  0xb2e 0xff ->  0x0 Link Ctl, ACK1
```

By excluding FSPF `hellos` and `ACK1`, you can focus on the frames of interest. See Example 29-7.

Example 29-7 Displays All VSAN 1 Traffic Excluding FSPF Hellos and ACK1 Frames.

```
switch(config)# fcan lo bri dis
(mdshdr.vsan==0x01)&&not((swils.opcode==0x14)or(fc.r_ctl==0xc0))
Capturing on eth2
10.589934   ff.fc.79 -> ff.fc.7a   FC-FCS 1    0x1b23 0xffff 0xff ->  0x0 GCAP
10.591253   ff.fc.7a -> ff.fc.79   FC-FCS 1    0x1b23 0x2f70  0x4 ->  0xf MSG_RJT (GCAP)
25.277981   ff.fc.79 -> ff.fc.7a   SW_ILS 1    0x1b27 0xffff 0xff ->  0x0 SW_RSCN
25.278050   ff.fc.79 -> ff.fc.89   SW_ILS 1    0x1b28 0xffff 0xff ->  0x0 SW_RSCN
25.279232   ff.fc.89 -> ff.fc.79   SW_ILS 1    0x1b28 0xadd7  0x5 ->  0xf SW_ACC (SW_RSCN)
25.280023   ff.fc.7a -> ff.fc.79   Unzoned NS 1    0x3b2b 0xffff  0x5 ->  0xf GE_PT
25.280029   ff.fc.7a -> ff.fc.79   SW_ILS 1    0x1b27 0x2f71  0x4 ->  0xf SW_ACC (SW_RSCN)
25.282439   ff.fc.79 -> ff.fc.7a   dNS    1    0x3b2b 0x1b29 0xff ->  0x0 RJT (GE_PT)
38.249966   00.00.00 -> ff.ff.fe   FC ELS 1    0x36f0 0xffff  0x3 ->  0xf FLOGI
38.262622   ff.ff.fe -> 79.03.00   FC ELS 1    0x36f0 0x1b2b 0xff ->  0x0 ACC (FLOGI)
38.262844   79.03.00 -> ff.ff.fc   FC ELS 1    0x3708 0xffff  0x3 ->  0xf PLOGI
38.262984   ff.ff.fc -> 79.03.00   FC ELS 1    0x3708 0x1b2c 0xff ->  0x0 ACC (PLOGI)
38.262851   79.03.00 -> ff.ff.fd   FC ELS 1    0x3720 0xffff  0x3 ->  0xf SCR
38.263514   ff.fc.79 -> ff.fc.7a   SW_ILS 1    0x1b2e 0xffff 0xff ->  0x0 SW_RSCN
38.263570   ff.fc.79 -> ff.fc.89   SW_ILS 1    0x1b2f 0xffff 0xff ->  0x0 SW_RSCN
38.263630   79.03.00 -> ff.ff.fc   dNS    1    0x3738 0xffff  0x3 ->  0xf GNN_FT
38.263884   ff.ff.fd -> 79.03.00   FC ELS 1    0x3720 0x1b2d 0xff ->  0x0 ACC (SCR)
38.264066   ff.fc.89 -> ff.fc.79   SW_ILS 1    0x1b2f 0xaddf  0x5 ->  0xf SW_ACC (SW_RSCN)
38.264417   ff.fc.89 -> ff.fc.79   dNS    1    0xade0 0xffff  0x5 ->  0xf GE_ID
38.264585   ff.fc.79 -> ff.fc.89   dNS    1    0xade0 0x1b31 0xff ->  0x0 ACC (GE_ID)
38.265132   ff.ff.fc -> 79.03.00   dNS    1    0x3738 0x1b30 0xff ->  0x0 ACC (GNN_FT)
38.265210   ff.fc.7a -> ff.fc.79   Unzoned NS 1    0x3b2f 0xffff  0x5 ->  0xf GE_PT
38.265414   79.03.00 -> ff.ff.fc   dNS    1    0x3750 0xffff  0x3 ->  0xf GPN_ID
38.265502   ff.fc.7a -> ff.fc.79   SW_ILS 1    0x1b2e 0x2f73  0x4 ->  0xf SW_ACC (SW_RSCN)
38.267196   ff.fc.79 -> ff.fc.7a   dNS    1    0x3b2f 0x1b32 0xff ->  0x0 ACC (GE_PT)
```

Use this command to focus on TE port initialization. This example allows two VSANs on the TE port and the port VSAN is 666. Hence the ELP, ESC, and EPP (0x71) go out on VSAN 666. Once the EPP negotiation is complete, we see EFP, DIA, RDI, MR, FSPF, and other updates flow for each allowed VSAN. See Example 29-8.

Example 29-8 Displays SW_ILS Traffic Between Fabric Controllers for all VSANs and Exclude FSPF Hellos and ACK1 Frames.

```
switch(config)# fcan lo bri dis
((fc.s_id==\”ff.ff.fd\”)&&(fc.type==0x22))&&not(swils.opcode==0x14)
Capturing on eth2
20.573225   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x200c 0xffff  0xe ->  0xf ELP
20.574021   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x200c 0xacc4 0xff ->  0x0 SW_ACC (ELP)
20.606020   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x200d 0xffff  0xe ->  0xf ESC
20.606232   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x200d 0xacc5 0xff ->  0x0 SW_ACC (ESC)
20.606665   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x200e 0xffff  0xe ->  0xf 0x71
20.608768   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x200e 0xacc6 0xff ->  0x0 SW_ACC (0x71)
20.615346   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0xacc7 0xffff 0xff ->  0x0 0x71
20.620330   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0xacc7 0x200f  0xe ->  0xf SW_ACC (0x71)
20.623028   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x2010 0xffff  0xe ->  0xf EFP
20.624681   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0xacc9 0xffff 0xff ->  0x0 EFP
20.624974   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x2010 0xacc8 0xff ->  0x0 SW_ACC (EFP)
20.625133   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0x1939 0xffff 0xff ->  0x0 EFP
20.626393   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0xacc9 0x2011  0xe ->  0xf SW_ACC (EFP)
20.627185   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0xab0b 0xffff  0xe ->  0xf EFP
20.627479   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0x1939 0xab0a  0xe ->  0xf SW_ACC (EFP)
20.627773   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0xab0c 0xffff  0xe ->  0xf DIA
20.631106   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0xab0b 0x193a 0xff ->  0x0 SW_ACC (EFP)
20.631432   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0xab0d 0xffff  0xe ->  0xf MR
20.631567   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0x193c 0xffff 0xff ->  0x0 DIA
20.631974   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0xab0c 0x193b 0xff ->  0x0 SW_ACC (DIA)
20.631938   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0x193c 0xab0e  0xe ->  0xf SW_ACC (DIA)
20.639262   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0x193e 0xffff 0xff ->  0x0 MR
20.640417   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0x193e 0xab0f  0xe ->  0xf SW_ACC (MR)
20.640598   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0xab0d 0x193d 0xff ->  0x0 SW_ACC (MR)
20.646950   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0xab14 0xffff  0xe ->  0xf LSU
20.647256   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0x1944 0xffff 0xff ->  0x0 LSU
20.647996   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0x1945 0xffff 0xff ->  0x0 LSU
20.648367   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0x1946 0xffff 0xff ->  0x0 LSA
20.648476   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0xab17 0xffff  0xe ->  0xf LSU
20.648916   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0xab19 0xffff  0xe ->  0xf LSA
20.649210   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0xab1a 0xffff  0xe ->  0xf LSA
20.659781   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0x194a 0xffff 0xff ->  0x0 LSA
20.660535   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0xab1d 0xffff  0xe ->  0xf LSU
20.660649   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0x194c 0xffff 0xff ->  0x0 LSU
20.660683   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0xab1e 0xffff  0x5 ->  0xf LSU
20.661006   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0x194e 0xffff 0xff ->  0x0 LSU
20.664994   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0xab22 0xffff  0xe ->  0xf LSA
20.665341   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0xab24 0xffff  0x5 ->  0xf LSU
20.665645   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0xab25 0xffff  0x5 ->  0xf LSA
20.666115   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0x1952 0xffff 0xff ->  0x0 LSA
20.666445   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0x1953 0xffff 0xff ->  0x0 LSU
20.666994   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0x1954 0xffff 0xff ->  0x0 LSA
20.667423   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0xab2a 0xffff  0x5 ->  0xf LSA
20.667715   ff.ff.fd -> ff.ff.fd   SW_ILS 1    0x1956 0xffff 0xff ->  0x0 LSA
30.525363   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x2012 0xffff  0xe ->  0xf DIA
30.525596   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x2012 0xacca 0xff ->  0x0 SW_ACC (DIA)
30.525959   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0xaccb 0xffff 0xff ->  0x0 RDI
30.526736   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0xaccb 0x2013  0xe ->  0xf SW_ACC (RDI)
30.527032   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x2014 0xffff  0xe ->  0xf EFP
30.527662   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x2014 0xaccc 0xff ->  0x0 SW_ACC (EFP)
30.533157   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x2015 0xffff  0xe ->  0xf MR
30.534159   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0xacce 0xffff 0xff ->  0x0 MR
30.534440   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x2015 0xaccd 0xff ->  0x0 SW_ACC (MR)
30.534791   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0xacce 0x2016  0xe ->  0xf SW_ACC (MR)
30.540883   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x201b 0xffff  0xe ->  0xf LSU
30.541068   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0xacd4 0xffff 0xff ->  0x0 LSU
30.541704   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0xacd5 0xffff 0xff ->  0x0 LSA
30.541981   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0xacd6 0xffff 0xff ->  0x0 LSU
```

```
30.542087   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x201e 0xffff  0xe ->  0xf LSA
30.542381   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x2020 0xffff  0xe ->  0xf LSU
30.542675   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x2021 0xffff  0xe ->  0xf LSU
30.542969   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x2022 0xffff  0xe ->  0xf LSA
30.543226   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0xacdb 0xffff 0xff ->  0x0 LSU
30.543614   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x2024 0xffff  0xe ->  0xf LSA
30.543751   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0xacdd 0xffff 0xff ->  0x0 LSA
30.544004   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0xacde 0xffff 0xff ->  0x0 LSA
30.544522   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0xacdf 0xffff 0xff ->  0x0 LSU
30.544553   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x2027 0xffff  0xe ->  0xf LSU
30.550961   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0xace7 0xffff 0xff ->  0x0 LSA
30.550988   ff.ff.fd -> ff.ff.fd   SW_ILS 666  0x202f 0xffff  0xe ->  0xf LSA
```

This example focuses on zone server changes. Prior knowledge of the domain controller ID is required. The switch domain ID where the fcanalyzer is run is x79, the domain controller is FF.FC.79. See Example 29-9.

Example 29-9 Display SW_ILS Traffic Between Fabric Domain Controllers for VSAN 1

```
switch(config)# fcan lo bri dis
mdshdr.vsan==0x01&&(fc.type==0x22)&&((fc.d_id==\”ff.fc.79\”\|\|fc.s_id==\"ff.fc.79\"))
Capturing on eth2
64.053927   ff.fc.79 -> ff.fc.7a   SW_ILS 1    0x1e15 0xffff 0xff ->  0x0 ACA
64.053995   ff.fc.79 -> ff.fc.89   SW_ILS 1    0x1e16 0xffff 0xff ->  0x0 ACA
64.054599   ff.fc.89 -> ff.fc.79   SW_ILS 1    0x1e16 0xb1e2  0x5 ->  0xf SW_ACC (ACA)
64.054747   ff.fc.7a -> ff.fc.79   SW_ILS 1    0x1e15 0x3037  0x4 ->  0xf SW_ACC (ACA)
64.057643   ff.fc.79 -> ff.fc.7a   SW_ILS 1    0x1e17 0xffff 0xff ->  0x0 SFC
64.057696   ff.fc.79 -> ff.fc.89   SW_ILS 1    0x1e18 0xffff 0xff ->  0x0 SFC
64.058788   ff.fc.7a -> ff.fc.79   SW_ILS 1    0x1e17 0x3038  0x5 ->  0xf SW_ACC (SFC)
64.059288   ff.fc.89 -> ff.fc.79   SW_ILS 1    0x1e18 0xb1e3  0x5 ->  0xf SW_ACC (SFC)
64.062011   ff.fc.79 -> ff.fc.7a   SW_ILS 1    0x1e19 0xffff 0xff ->  0x0 UFC
64.062060   ff.fc.79 -> ff.fc.89   SW_ILS 1    0x1e1a 0xffff 0xff ->  0x0 UFC
64.073513   ff.fc.7a -> ff.fc.79   SW_ILS 1    0x1e19 0x3039  0x5 ->  0xf SW_ACC (UFC)
64.765306   ff.fc.89 -> ff.fc.79   SW_ILS 1    0x1e1a 0xb1e4  0x5 ->  0xf SW_ACC (UFC)
64.765572   ff.fc.79 -> ff.fc.7a   SW_ILS 1    0x1e1b 0xffff 0xff ->  0x0 RCA
64.765626   ff.fc.79 -> ff.fc.89   SW_ILS 1    0x1e1c 0xffff 0xff ->  0x0 RCA
64.766386   ff.fc.7a -> ff.fc.79   SW_ILS 1    0x1e1b 0x303a  0x4 ->  0xf SW_ACC (RCA)
64.766392   ff.fc.89 -> ff.fc.79   SW_ILS 1    0x1e1c 0xb1e5  0x5 ->  0xf SW_ACC (RCA)
```

Capture Filters

You can limit what frames are captured 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 are useful in restricting the amount of bandwidth consumed by the remote capture.

Unlike display filters, capture filters restrict a capture to the specified frames. No other frames are 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 documented in the Ethereal website (http://www.ethereal.com). Some examples of how you can use this feature as follows:

- 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

This section lists the 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 WWNs 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 29-1).

Table 29-1 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 world-wide names should be made by an administrator or individual who is completely familiar with switch operations.

Configuring a Secondary MAC Address

To allocate secondary MAC addresses, follow these steps:

	Command	Purpose

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

Step 2	`switch(config)# wwn 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 29-10 to 29-12.

Example 29-10 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 29-11 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 29-12 Displays the WWN for a Specific Switch

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

Allocating Flat FC IDs

Fibre Channel standards require a unique FC ID to be allocated to an 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 an 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 mode. In the auto mode, only HBAs without interop issues are assigned FCIDs with specific port 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.

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`	Allocates one area to the N port attached to an F port.
	`switch(config)# fcinterop fcid-allocation flat`	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`	Intelligently assigns flat FC ID to N ports that can interoperate in **flat** mode, otherwise assigns full area to all other ports. This is the default.

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

Enabling Loop Monitoring

By default, the loop monitoring is disabled in all switches in the Cisco MDS 9000 Family. 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).

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

The **fcinterop loop-monitor** command enables loop polling for FL ports in a Cisco MDS 9000 Family switch.

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.

Configuring the Switch for Interoperability

Interoperability enables the products of multiple vendors to 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 provides the product with a more aimiable standards compliant implementation.

Table 29-2 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 29-2 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 McData’s nominal restriction to this same range. They can either be set up statically (the Cisco MDS switch accept only 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, D_S_TOV, E_D_TOV, and R_A_TOV.
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. **Note** Brocade uses the **cfgsave** command to save fabric-wide zoning configuration. This command does not 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.
Zone propagation	Some vendors do not pass the full zone configuration to other switches, only the active zone set gets passed. Verify that the active zone set or zone configuration has correctly propagated to the other switches in the fabric.
VSAN	Interop mode only affects the specified VSAN.

Table 29-2 Changes in Switch Behavior When Interoperability Is Enabled (continued)

Switch Feature	Changes if Interoperability Is Enabled
TE ports and PortChannels	TE ports and PortChannels cannot be used to connect Cisco MDS to non-Cisco MDS switches. Only E ports can be used to connect to non-Cisco MDS switches. TE ports and PortChannels can still be used to connect an Cisco MDS to other Cisco 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.

Note 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 or McData switches do not understand. Rejecting these frames, causes the common E ports to become isolated.

To configure interoperability in any switch in the Cisco MDS 9000 Family, 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 1
```

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 principal switch. If the **preferred** option is used, Cisco MDS 9000 switches request a specific ID, but still join the fabric if the principal switch assigns a different ID. If the **static** option is used, the Cisco MDS 9000 switches do not join the fabric unless the principal switch agrees, and assigns the requested ID.

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

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

Note The Cisco 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 Cisco MDS domain manager function for the altered VSAN.

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

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

or

- Do not 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.

To verify the resulting status of issuing the interoperability command in any switch in the Cisco MDS 9000 Family, follow these steps:

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

```
switch# show version
Cisco Storage Area Networking Operating System (SAN-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2003, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
Andiamo Systems, Inc. and/or other third parties and are used and
distributed under license. Some parts of this software are covered
under the GNU Public License. A copy of the license is available
at http://www.gnu.org/licenses/gpl.html.

Software
```

```
  BIOS:      version 1.0.8
  loader:    version 1.1(2)
  kickstart: version 2.0(1) [build 2.0(0.6)] [gdb]
  system:    version 2.0(1) [build 2.0(0.6)] [gdb]

  BIOS compile time:       08/07/03
  kickstart image file is: bootflash:///m9500-sf1ek9-kickstart-mzg.2.0.0.6.bin
  kickstart compile time:  10/25/2010 12:00:00
  system image file is:    bootflash:///m9500-sf1ek9-mzg.2.0.0.6.bin
  system compile time:     10/25/2020 12:00:00


Hardware
  RAM 1024584 kB

  bootflash: 1000944 blocks (block size 512b)
  slot0:           0 blocks (block size 512b)

  172.22.92.181 uptime is 0 days 2 hours 18 minute(s) 1 second(s)

  Last reset at 970069 usecs after Tue Sep 16 22:31:25 1980
    Reason: Reset Requested by CLI command reload
    System version: 2.0(0.6)
    Service:
```

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 Cisco MDS name server shows both local and remote entries, and does not time out the entries.

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 varies 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 manual scrolling. Use the **show terminal** command to view the configured the terminal size. After obtaining the output of this command, remember to reset you terminal length as required (see the "Setting the Terminal Length" section on page 2-16).

Tip You can save the output of this command to a file by appending **>** *filename* to the **show tech-support** command (see the "Saving Command Output to a File" section on page 2-23). 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 (see the "Compressing and Uncompressing Files" section on page 2-23). Copy the zipped file to the required location using the **copy** command and unzip the file using the **gunzip** command (see the "Copying Files" section on page 2-22).

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.

Using the show tech-support brief Command

Use the **show tech-support brief** command to obtain a quick, condensed review of your switch configurations. This command provides a summary of the current running state of the switch.

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

Tip You can save the output of this command to a file by appending **>** *filename* to the **show tech-support brief** command (see the "Saving Command Output to a File" section on page 2-23).

Example 29-13 Displays the Condensed View of Switch Configurations

```
vegas01# show tech-support brief
Switch Name           : vegas01
Switch Type           : DS-X9216-K9-SUP
Kickstart Image       : 1.3(2) bootflash:///m9200-ek9-kickstart-mz.1.3.1.10.bin
System Image          : 1.3(2) bootflash:///m9200-ek9-mz.1.3.1.10.bin
IP Address/Mask       : 10.76.100.164/24
Switch WWN            : 20:00:00:05:30:00:84:9e
No of VSANs           : 9
Configured VSANs      : 1-6,4091-4093

VSAN    1:    name:VSAN0001, state:active, interop mode:default
              domain id:0x6d(109), WWN:20:01:00:05:30:00:84:9f [Principal]
              active-zone:VR, default-zone:deny

VSAN    2:    name:VSAN0002, state:active, interop mode:default
              domain id:0x7d(125), WWN:20:02:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny

VSAN    3:    name:VSAN0003, state:active, interop mode:default
              domain id:0xbe(190), WWN:20:03:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny

VSAN    4:    name:VSAN0004, state:active, interop mode:default
              domain id:0x5a(90), WWN:20:04:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny

VSAN    5:    name:VSAN0005, state:active, interop mode:default
              domain id:0x13(19), WWN:20:05:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny

VSAN    6:    name:VSAN0006, state:active, interop mode:default
              domain id:0x1f(31), WWN:20:06:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny

VSAN 4091:    name:VSAN4091, state:active, interop mode:default
              domain id:0x08(8), WWN:2f:fb:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny

VSAN 4092:    name:VSAN4092, state:active, interop mode:default
              domain id:0x78(120), WWN:2f:fc:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny

VSAN 4093:    name:VSAN4093, state:active, interop mode:default
              domain id:0x77(119), WWN:2f:fd:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny
```

```
-------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          FCOT   Oper  Oper   Port
                  Mode   Trunk                          Mode  Speed  Channel
                         Mode                                 (Gbps)
-------------------------------------------------------------------------------
fc1/1      1      auto   on      fcotAbsent       --     --           --
fc1/2      1      auto   on      fcotAbsent       --     --           --
fc1/3      1      auto   on      fcotAbsent       --     --           --
fc1/4      1      auto   on      fcotAbsent       --     --           --
fc1/5      1      auto   on      notConnected     swl    --           --
fc1/6      1      auto   on      fcotAbsent       --     --           --
fc1/7      1      auto   on      fcotAbsent       --     --           --
fc1/8      1      auto   on      fcotAbsent       --     --           --
fc1/9      1      auto   on      fcotAbsent       --     --           --
fc1/10     1      auto   on      fcotAbsent       --     --           --
fc1/11     1      auto   on      fcotAbsent       --     --           --
fc1/12     1      auto   on      fcotAbsent       --     --           --
fc1/13     1      auto   on      fcotAbsent       --     --           --
fc1/14     1      auto   on      fcotAbsent       --     --           --
fc1/15     1      auto   on      fcotAbsent       --     --           --
fc1/16     1      auto   on      fcotAbsent       --     --           --

-------------------------------------------------------------------------------
Interface          Status                             Speed
                                                      (Gbps)
-------------------------------------------------------------------------------
sup-fc0            up                                 1

-------------------------------------------------------------------------------
Interface               Status     IP Address        Speed        MTU
-------------------------------------------------------------------------------
mgmt0                   up         10.76.100.164/24  100 Mbps     1500
```

Default Settings

Table 29-3 lists the default settings for the features included in this chapter.

Table 29-3 Default Settings for Advanced Features

Parameters	Default
D_S_TOV	5,000 milliseconds.
E_D_TOV	2,000 milliseconds.
R_A_TOV	10,000 milliseconds.
Timeout period to invoke fctrace	5 seconds.
Number of frame sent by the fcping feature	5 frames.
Remote capture connection protocol	TCP.
Remote capture connection mode	Passive.
Local capture frame limit s	10 frames.
FC ID allocation mode	Auto mode.

Table 29-3 Default Settings for Advanced Features (continued)

Parameters	Default
Loop monitoring	Disabled.
Default output of the **show tech-support** command	The output of the **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**, and **show flash** commands.