CHAPTER 49

Troubleshooting Your Fabric

This chapter describes basic troubleshooting methods used to resolve issues with switches. This chapter includes the following sections:

- The fctrace Feature, page 49-1
- The fcping Feature, page 49-3
- Configuring a Fabric Analyzer, page 49-4
- Loop Monitoring Initiation, page 49-14
- The show tech-support Command, page 49-14

The fctrace Feature

-
- Compute inter-switch (hop-to-hop) latency.

You can invoke fctrace by providing the FC ID, the N port, or the NL port WWN, or the device alias 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)	
	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)	By default the period to wait before timing out is 5 seconds, The range is from one through 10 seconds.
	fctrace device-alias disk1 v 1	

The fcping Feature

	Command	Purpose
Step 1	**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	
	switch# 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	from 0 through 2147483647. A value of 0 pings forever.
	fcping fcid 0xd500b4 vsan 1 timeout 10	Sets the timeout value. The default period to wait is 5 seconds. The range is from 1 through 10 seconds.
	fcping device-alias disk1 vsan 1	Invokes fcping for the specified device alias of the destination.
Step 2	**fcping fcid 0x010203 vsan 1** No response from the N port. switch# 28 bytes from 21:00:00:20:37:6f:db:dd time = 1454 usec ... 5 frames sent, 5 frames received, 0 timeouts Round-trip min/avg/max = 364/784/1454 usec	No response from the N port Retry the command a few seconds later.

Verifying Switch Connectivity

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:

show fcdomain domain-list vsan 200 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 (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.
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	

Configuring a Fabric Analyzer

- libpcap—See http://www.tcpdump.org.

  Ethereal—See http://www.ethereal.com.

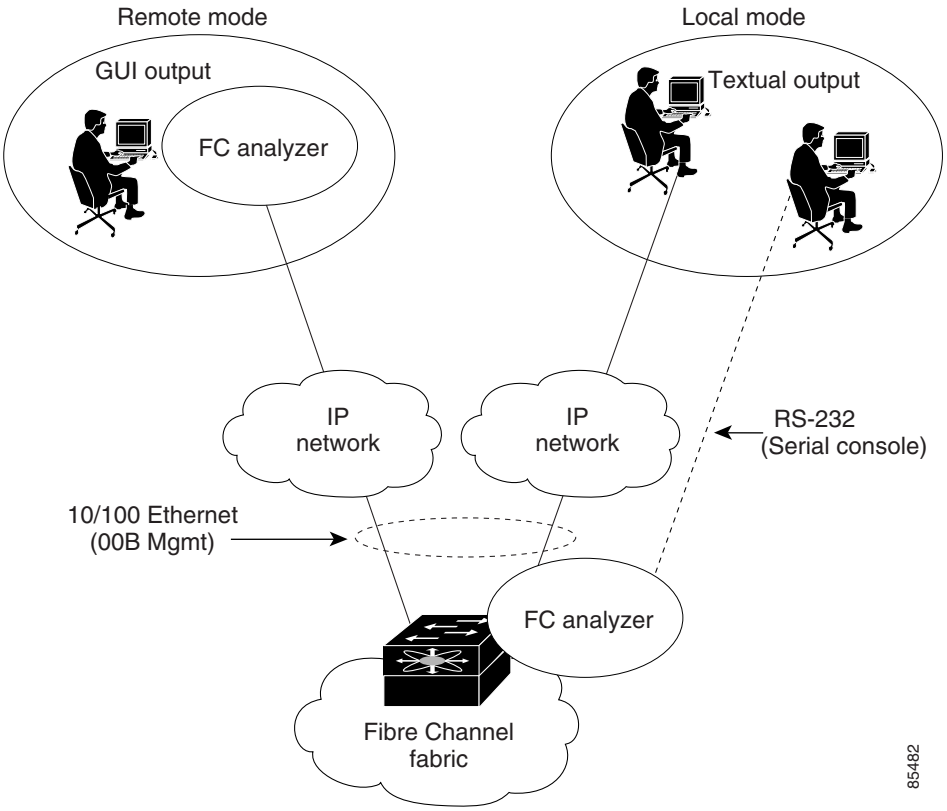
The Cisco Fabric Analyzer is useful in capturing and decoding control traffic, not data traffic. It is suitable for control path captures, and is not intended for high-speed data path captures.

About the Cisco Fabric Analyzer

-
  -
  -

  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 49-1 Cisco Fabric Analyzer Usage



Local Text-Based Capture

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 49-7.

Remote Capture Daemon

-
-

GUI-Based Client

Configuring the Cisco Fabric Analyzer

-
-

Capturing Frames Locally

	Command	Purpose
Step 1		
	Note	
Step 2	`fcanalyzer local`	
	`fcanalyzer local brief`	
	`fcanalyzer local display-filter SampleF`	
	`fcanalyzer local limit-frame-size 64`	
	`fcanalyzer local limit-captured-frames 10`	
	Ctrl-c **fcanalyzer local limit-captured-frames** *number*	
Step 3		**Note**

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

	Command	Purpose
Step 1		
Step 2	**fcanalyzer remote 10.21.0.3**	
	fcanalyzer remote 10.21.0.3 active	
	fcanalyzer remote 10.21.0.3 active 1	

-

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

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

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

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

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

Start **Run**

Clearing Configured fcanalyzer Information

Displaying Configured Hosts

show fcanalyzer

Example 49-1 Displays Configured Hosts

```
ActiveClient = 10.21.0.3, DEFAULT
```

```
    mdshdr.vsan == 2

    fcswils

    mdshdr.sof == SOFf

    swils.opcode == HLO || swils.opcode == LSU || swils.opcode == LSA

    fcels.opcode == FLOGI

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

    dNS
```

Defining Display Filters

-
-
-
-
-

Note

Displaying Filters Examples

brief

Example 49-2 Displays Only Fabric Login Server Traffic on VSAN 1

```
(mdshdr.vsan==0x01)&&((fc.d_id==\"ff.ff.fe\"\|\|fc.s_id==\"ff.ff.fe\"))
```

show flogi database interfac

Example 49-3 Displays All Traffic for a Particular N Port on VSAN 1

```
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)
```

Example 49-4 Displays All Traffic for a Specified VSAN

```
switch(config)#
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

                hellos    ACK1
```

Example 49-5 Displays All VSAN 1 Traffic Excluding FSPF Hellos and ACK1 Frames.

```
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)
```

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 49-6.

Example 49-6 Displays SW_ILS Traffic Between Fabric Controllers for all VSANs and Exclude FSPF Hellos and ACK1 Frames.

```
Warning:Couldn't obtain netmask info (eth2:no IPv4 address assigned).
Capturing on eth2
9.472181 ff.fc.ef -> ff.fc.61 0x5e0a 0xffff SW_ILS ACA
9.472777 ff.fc.61 -> ff.fc.ef 0x5e0a 0x5e09 SW_ILS SW_ACC (ACA)
9.474551 ff.fc.ef -> ff.fc.61 0x5e0b 0xffff SW_ILS SFC
9.475706 ff.fc.61 -> ff.fc.ef 0x5e0b 0x5e0a SW_ILS SW_ACC (SFC)
9.476694 ff.fc.ef -> ff.fc.61 0x5e0c 0xffff SW_ILS UFC
9.483612 ff.fc.61 -> ff.fc.ef 0x5e0c 0x5e0b SW_ILS SW_ACC (UFC)
9.488187 ff.fc.ef -> ff.fc.61 0x5e0d 0xffff SW_ILS RCA
9.493703 ff.fc.61 -> ff.fc.ef 0x5e0d 0x5e0c SW_ILS SW_ACC (RCA)
```

Example 49-7 Display Switch Internal Link Services (SW_ILS) Traffic To and From Fabric Domain Controller ff.fc.79

show fcs ie vsan

```
IE List for VSAN:999
------------------------------------------------------------------------
IE-WWN                    IE-Type             Mgmt-Id         Mgmt-Addr
------------------------------------------------------------------------
23:e7:00:05:30:00:91:5f   Switch (Remote)     0xfffc04         10.66.78.51
23:e7:00:05:30:00:9b:9f   Switch (Adjacent)   0xfffc01         10.66.78.52
23:e7:00:0d:ec:00:93:81   Switch (Local)      0xfffc79         10.66.78.54
[Total 3 IEs in Fabric]
```

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:

To capture only class F frames, use this expression:

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

To capture only name server frames, use this expression:

To capture only SCSI command frames, use this expression:

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

This section lists the permitted capture filters.

```
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
```

Loop Monitoring Initiation

Caution

	Command	Purpose
Step 1		Enters configuration mode.
Step 2		Enables the loop monitoring feature.
		Disables (default) the loop monitoring feature and reverts the switch to the factory defaults.

The show tech-support Command

EXEC mode to display general information about the switch when reporting a problem.

Note

Tip > *filename*

filename

Cisco MDS 9000 Family Configuration Guide *Cisco MDS 9000 Family Command Reference* *Cisco MDS 9000 Family Troubleshooting Guide*

The show tech-support brief Command

Tip

Example 49-8 Displays the Condensed View of Switch Configurations

```
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
```