Contents

Troubleshooting Ports

This section describes how to identify and resolve problems that can occur with ports in the Cisco MDS 9000 Family of multilayer directors and fabric switches. It includes the following sections:

- Overview
- Initial Troubleshooting Checklist
- Overview of the FC-MAC Driver and the Port Manager
- Common Problems with Port Interfaces

Overview

Before a switch can relay frames from one data link to another, the characteristics of the interfaces through which the frames are received and sent must be defined. The configured interfaces can be Fibre Channel interfaces, Gigabit Ethernet interfaces, the management interface (mgmt0), or VSAN interfaces (IPFC).

Each physical Fibre Channel interface in a switch can operate in one of several port modes: E port, F port, FL port, TL port, TE port, SD port, and B port. In addition to these modes, each interface can be configured in auto or Fx port modes. These modes determine the port type during interface initialization.

Each interface has an associated administrative configuration and operational status:

- The administrative configuration does not change unless you modify it. This configuration has various attributes that you can configure in administrative mode.
- The operational status represents the current status of a specified attribute such as the interface speed. This status cannot be changed and is read-only. Some values may not be valid when the interface is down (such as the operation speed).

For a complete description of port modes, administrative states, and operational states, refer to the *Cisco MDS 9000 Family Configuration Guide* and the *Cisco MDS 9000 Fabric Manager Configuration Guide.*

Initial Troubleshooting Checklist

Troubleshooting a SAN problem involves gathering information about the configuration and connectivity of individual devices and the entire SAN fabric. In the case of port interfaces, begin your troubleshooting activity as follows:

Checklist	Check off
Check the physical media to ensure there are no damaged parts.	
Verify that the SFP (small form-factor pluggable) devices in use are those authorized by Cisco and that they are not faulty.	
Verify that you have enabled the port by right-clicking the port in Device Manager and selecting **enable** or by using the **no shut** CLI command.	
Right-click the port in Device Manager or use the **show interface** CLI command to verify the state of the interface. Refer to **Table 8-1** for reasons why a port may be in a down operational state.	
Verify that you if you have one host-optimized port configured as an ISL, you have not connected to the other three ports in the port group.	

Verify that no ports on a Generation 2 module are out of service.

Note: Use the **show running interface** CLI command to view the interface configuration in Cisco SAN-OS Release 3.0(1) or later. The interface configuration as seen in the **show running-config** CLI command output is no longer consolidated.

Table 8-1 Reason Codes for Nonoperational States

Reason Code	Description	Applicable Mode
Link failure or not connected	The physical layer link is not operational.	All
SFP not present	The small form-factor pluggable (SFP) hardware is not plugged in.	
Initializing	The physical layer link is operational and the protocol initialization is in progress.	
Reconfigure fabric in progress	The fabric is currently being reconfigured.	
Offline	The Cisco SAN-OS software waits for the specified R_A_TOV time before retrying initialization.	
Inactive	The interface VSAN is deleted or is in a suspended state. To make the interface operational, assign that port to a configured and active VSAN.	
Hardware failure	A hardware failure is detected.	
Error disabled	Error conditions require administrative attention. Interfaces may be error-disabled for various reasons. For example: • Configuration failure. • Incompatible buffer-to-buffer credit configuration. To make the interface operational, you must first fix the error conditions causing this state; then, administratively shut down and reenable the interface.	
Isolation due to ELP failure	The port negotiation failed.	Only E ports and TE ports
Isolation due to ESC failure	The port negotiation failed.	
Isolation due to domain overlap	The Fibre Channel domains (fcdomain) overlap.	
	The assigned domain ID is not valid.	

Isolation due to domain ID assignment failure		
Isolation due to other side E port isolated	The E port at the other end of the link is isolated.	
Isolation due to invalid fabric reconfiguration	The port is isolated due to fabric reconfiguration.	
Isolation due to domain manager disabled	The fcdomain feature is disabled.	
Isolation due to zone merge failure	The zone merge operation failed.	
Isolation due to VSAN mismatch	The VSANs at both ends of an ISL are different.	
Nonparticipating	FL ports cannot participate in loop operations. It may happen if more than one FL port exists in the same loop, in which case all but one FL port in that loop automatically enters nonparticipating mode.	Only FL ports and RL ports
PortChannel administratively down	The interfaces belonging to the PortChannel are down.	Only PortChannel interfaces
Suspended due to incompatible speed	The interfaces belonging to the PortChannel have incompatible speeds.	
Suspended due to incompatible mode	The interfaces belonging to the PortChannel have incompatible modes.	
Suspended due to incompatible remote switch WWN	An improper connection is detected. All interfaces in a PortChannel must be connected to the same pair of switches.	

Note: We recommend that you do not disable and then enable a T or TE port. This action can affect all of the VSANs crossing the EISL instead of only the VSAN experiencing the isolation problem.

Limitations and Restrictions

- You must administratively enable a port with the **no shut** command. When the interface is enabled, the administrative state of the port is up. If you administratively disable an interface with the **shut** command, the administrative state of the port is down, and the physical link layer state change is ignored.
- For a port to be in an up operational state where it can transmit or receive traffic, the interface must be administratively up, the interface link layer state must be up, and the interface initialization must be complete.
- The interface cannot transmit or receive data when a port's operational state is down.
- The interface is operating in TE mode when a port's operational state is trunking.

Overview of the FC-MAC Driver and the Port Manager

This section describes the internal details of port-related components in Cisco SAN-OS. Use this section to understand the underlying functions that might be causing port-related problems.

The FC-MAC driver resides in the module component of the Cisco MDS 9000 Family SAN-OS software. It performs the following functions:

- Initialization of FC-MAC ASIC
- Speed negotiation
- Link/loop port initialization and credit recovery
- Statistics collection
- Error handling (mainly by acting on error interrupts)
- SFP detection and housekeeping
- Statistics collection
- Debug command support under the **show hardware internal fc-mac** command on the module

The FC-MAC driver does not handle FLOGI, RSCN, or configuration management.

This section includes the following topics:

- Port Manager Overview
- Troubleshooting Port States with the Device Manager
- Isolating Port Issues Using Device Manager
- Using Port Debug Commands
- Useful Commands at the FC-MAC Level

Port Manager Overview

The Port Manager is management software running on the supervisor module. The Port Manager handles the following tasks:

- Port configuration management
- Link events, including notifying the registered application on the supervisor module
- E or TE port initialization
- SFP validation

The FC-MAC detects the port is in one of the following states:

- Disable--The port is administratively disabled.
- Enable--The port is administratively enabled. In this state, the port may be in speed initialization, loop-initialization, link (point-to-point connection) initialization, or the link-up state.
- HW Failure--The port has been declared bad due to a hardware failure.
- Pause--An intermediate state after the link is down and subsequent enabling of the port to start the port initialization.

You can check the state of the port by attaching to the module using this command:

show hardware internal fc-mac port *port* **port-info**

Note: You must use the **attach module** CLI command to access FC-MAC **show** commands.

The FLOGI server is a separate application that handles the FLOGI processing for Nx ports.

Troubleshooting Port States with the Device Manager

Device Manager offers multiple ways to monitor ports, including:

- Device View
- Summary View
- Port Selection
- Port Monitoring

Device View

Basic port monitoring using Device Manager begins with the visual display in the Device View (Figure 8-1). Port display descriptions include:

- Green box ? A successful fabric login has occurred; the connection is active.
- Red X ? A small form-factor pluggable transceiver (SFP) is present but there is no connection. This might indicate a disconnected or faulty cable, or no active device connection.
- Red box ? An FSP is present but fabric login (FLOGI) has failed. Typically there is a mismatch in port or fabric parameters with the neighboring device. For example, a port parameter mismatch occurs if a node device were connected to a port configured as an E port. An example of a fabric parameter mismatch is differing timeout values.
- Yellow box ? In Device Manager, a port was selected.
- Gray box ? The port is administratively disabled.
- Black box ? FSP is not present.

Figure 8-1 Device Manager: Device View
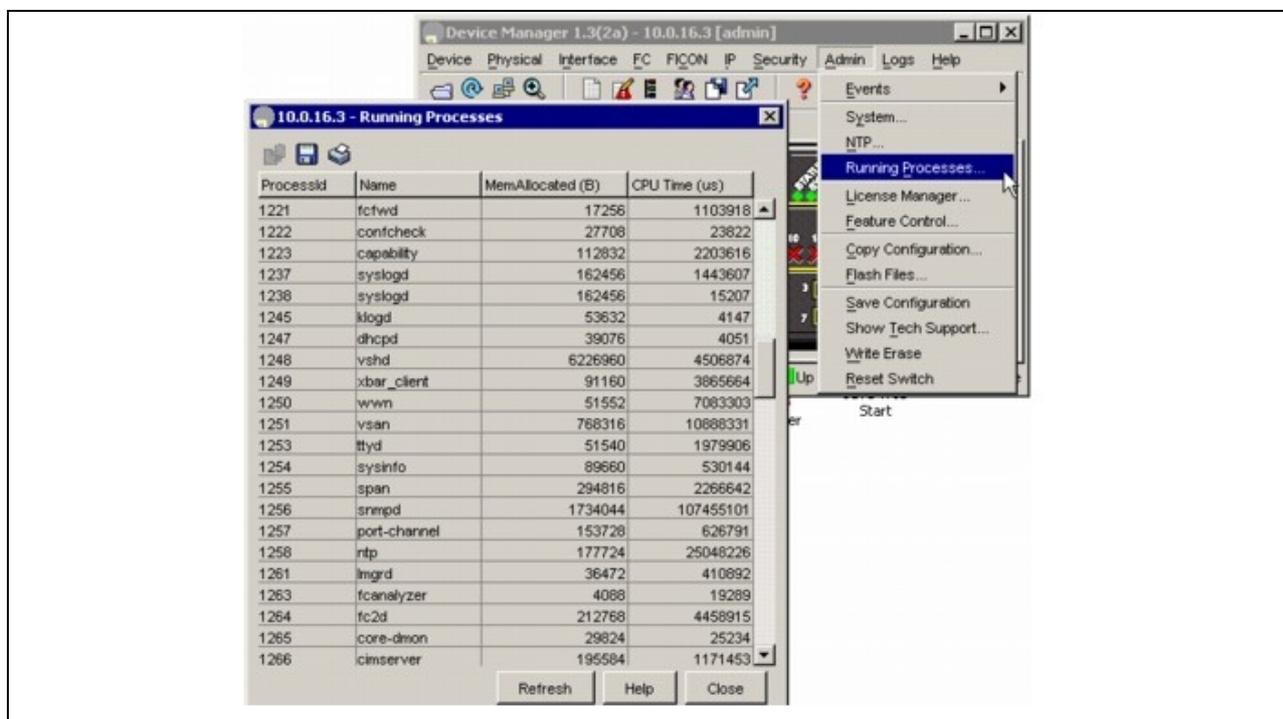
Device Manager: Summary View

In Device Manager, selecting the Summary View (Figure 8-2) expands on the information available for port monitoring. The display includes:
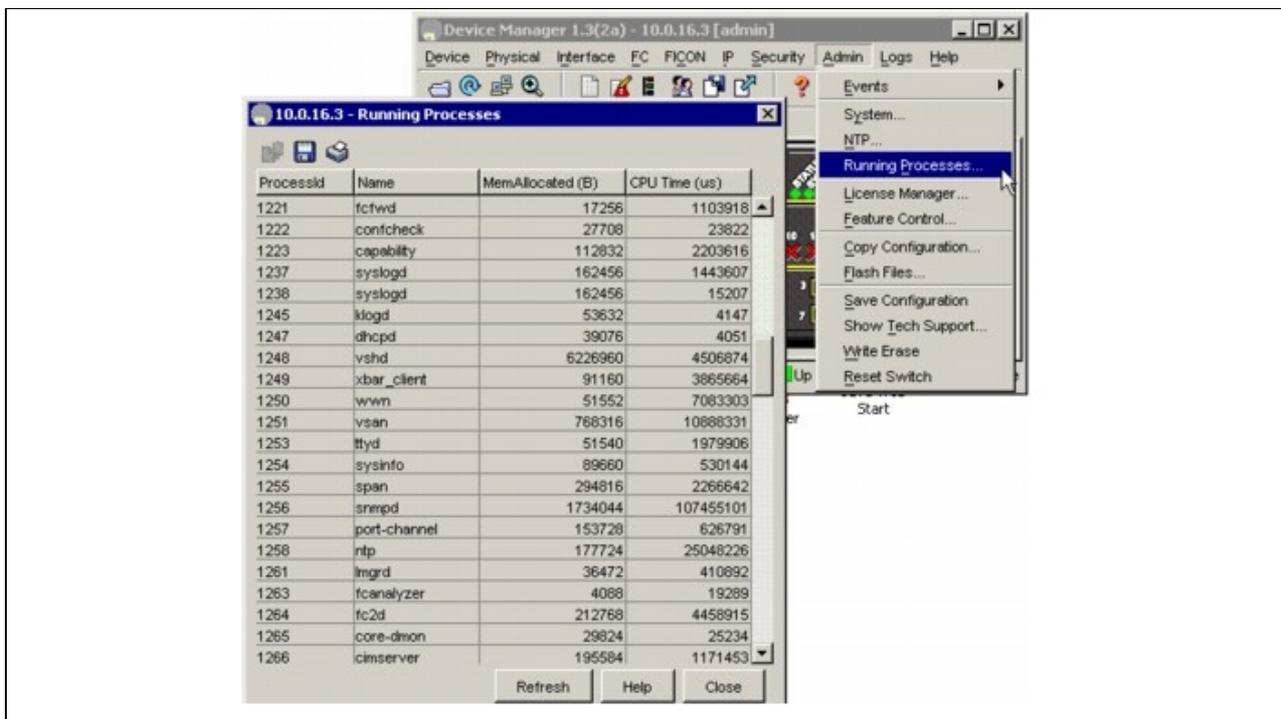
- VSAN assignment
- For N ports, the port world-wide name (pWWN) and Fibre Channel ID (FC ID) of the connected device
- For ISLs, the IP address of the connected switch
- Speed
- Frames transmitted and received
- Percent utilization for the CPU, dynamic memory, and flash memory

Figure 8-2 Device Manager: Summary View

Device Manager: Port Selection

To drill down for additional port information, use either the Device View or Summary View, and double-click any port. The initial display (Figure 8-3) shows administrative settings for Mode, Speed, and Status, plus current operational status, failure cause, and date of the last configuration change.

Additional tabs include:

- Rx BB Credit ?Configure and view buffer-to-buffer credits (BB credits).
- Other ? View PortChannel ID, WWN, maximum transmission unit (MTU), configure maximum receive buffer size.
- FLOGI ? View FC ID, pWWN, nWWN, BB credits and class of service for N port connections.
- ELP ? View pWWN, nWWN, BB credits and supported classes of service for ISLs.
- Trunk Config ? View and configure trunk mode and allowed VSANs.
- Trunk Failure ? Failure cause for ISLs.
- Physical ? Configure beaconing; view SFP information.

- Capability ? View current port capability for hold-down timers, BB credits, maximum receive buffer size.

Figure 8-3 Device Manager: Port Selection
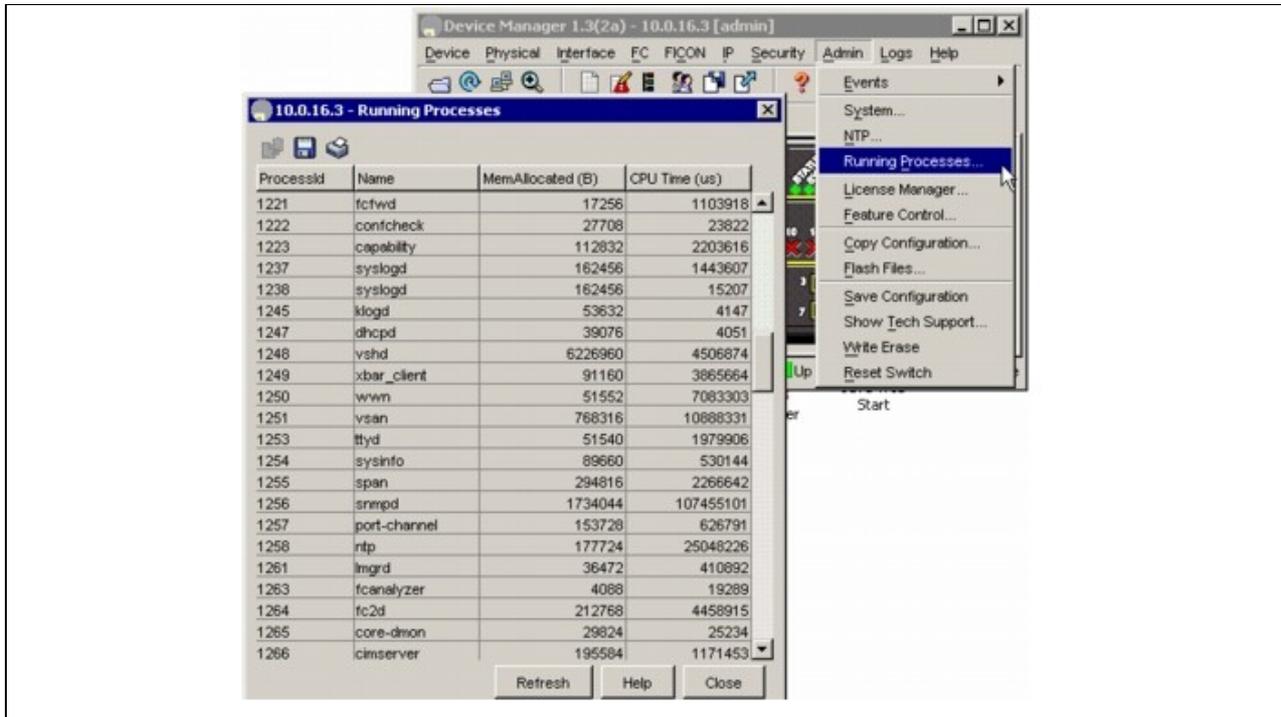
Device Manager: Port Monitoring

To display additional details about port traffic, use the Device View or Summary View. In Device View, choose one or more ports, right-click and choose **Monitoring** from the pop-up menu. In Summary View, choose one or more interfaces, and click the **Monitor** tool. The initial display (Figure 8-4) shows traffic information for the selected interval, including the number of bytes and frames received and transmitted.

Additional tabs include:

- Protocol ? View protocol-related traffic and error statistics, including link reset counts, offline and non-operational sequence errors, reset protocol errors, and statistics related to buffer-to-buffer flow control.
- Discards ? View the number of frames discarded by the port, including Class 2, Class 3, and Class F frames, EISL frames, and totals.
- Link Errors ? View the number of link errors, including link failures, signal losses, synchronization failures, invalid transmission words, and delimiter and address identifier errors.
- Frame Errors ? View frame error statistics, including the number of frames with invalid CRC, Class 3 frames that were discarded upon reception, FBSY returns for selected situations, and FRJT returns resulting from frame rejection by fabric.
- Class 2 Traffic ? View the amount of Class 2 traffic for the selected interval.
- Class 2 Errors ? View error statistics for Class 2 traffic, including busy frame responses and port rejects.
- FICON ? View FICON error statistics, including pacing, disparity, EOF, OOF, and order sets errors.

Figure 8-4 Device Manager: Port Monitoring Traffic Tab
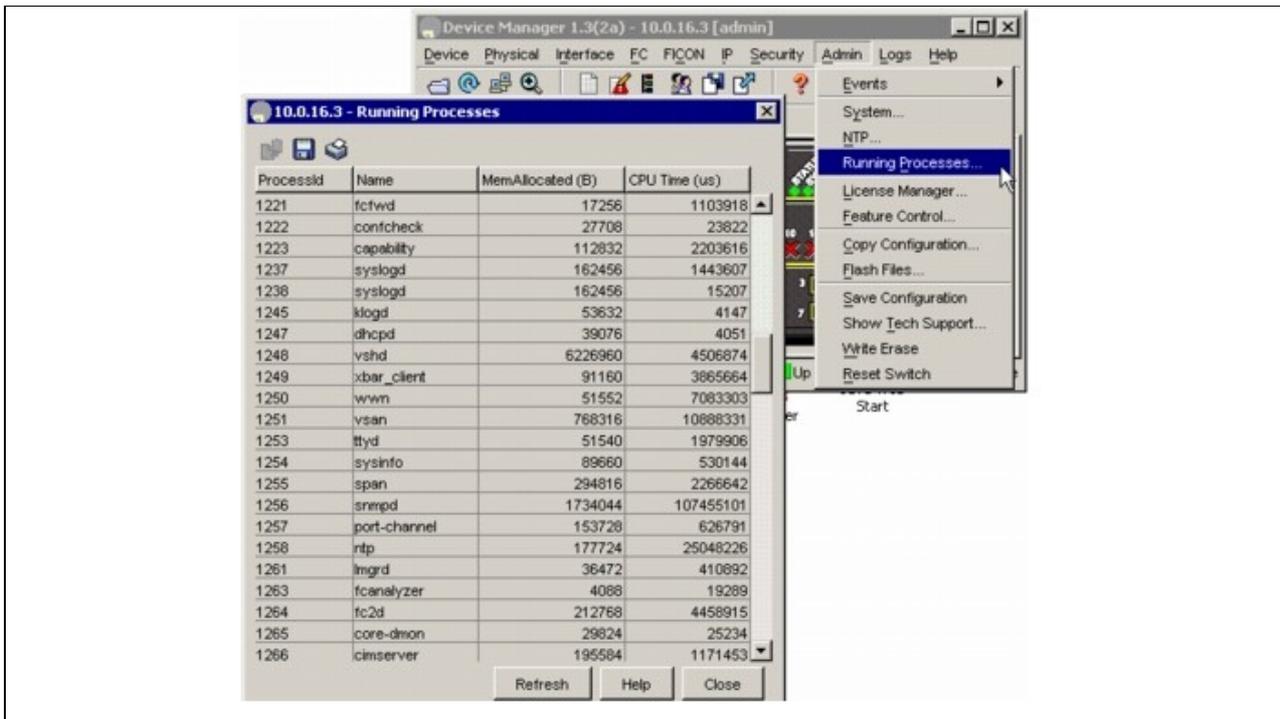
The port monitoring view also provide access to graphing tools. Select the cells that you are interested in, and then click one of the graphing tools to display the related line Figure 8-5), bar, area, or pie chart.

Figure 8-5 Device Manager: Port Monitoring Line Chart
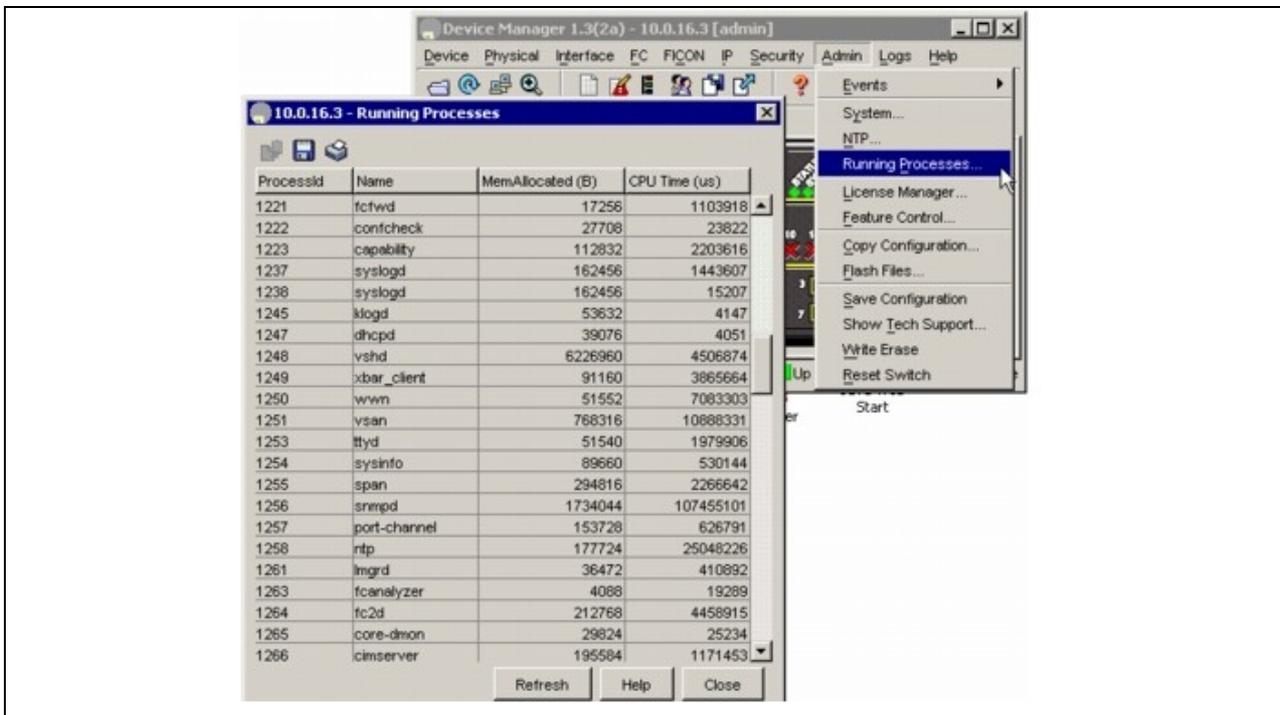
Isolating Port Issues Using Device Manager

To isolate port issues using Device Manager, follow these steps:

1. Choose **Interfaces > FC ALL** and verify that the Status Oper field is **up** to determine if the host HBA and the storage port can provide link level connectivity to their respective switches.

> See Table 8-1 for details on nonoperational interface reasons.

2. If the port is down and offline, set Admin Status to **up** and click **Apply** to bring the port online.

3. Repeat Step 1 to determine if the port is online.

> ◊ If either of the ports fails to remain in the online state, then you may have a faulty GBIC, cabling or HBA/subsystem port.

4. If both ports are online, click the **FLOGI** tab to verify that the Fibre Channel ports for the host and storage have performed a fabric login (FLOGI) and are communicating with their respective switches.

5. Choose **FC > Name Server** to verify that the assigned FC ID during FLOGI exists in the name server database.

At this point, the HBA and subsystem ports have successfully established link-level connectivity and each one can communicate with its locally attached switch in the fabric. The next step is to verify zone membership. For a more detailed discussion and description of VSANs and zones, see "Troubleshooting Zones and Zone Sets".

Troubleshooting Port States from the CLI

To display complete information for an interface, use the **show interface** command. In addition to the state of the port, this command displays:

- Port WWN
- Speed
- Trunk VSAN status
- Transmit and receive buffer-to-buffer credits configured and remaining
- Maximum receive buffer size
- Number of frames sent and received
- Transmission errors, including discards, errors, CRCs, and invalid frames

Example 8-1 displays the **show interface** command output.

Example 8-1 show interface Command Output

```
switch# show interface fc1/3
fc1/3 is trunking
Hardware is Fibre Channel, SFP is short wave laser
Port WWN is 20:03:00:0b:fd:8c:f8:80
Peer port WWN is 20:10:00:0b:fd:2c:8c:00
Admin port mode is auto, trunk mode is on
Port mode is TE
Port vsan is 161
Speed is 2 Gbps
Transmit B2B Credit is 255
Receive B2B Credit is 255
Receive data field Size is 2112
```

Using Port Debug Commands

Use the **show hardware internal debug-info interface fc** CLI command to debug ports.

Note: To enter commands with the **internal** keyword, you must have an account that is a member of the network-admin group.

Examples of when to use these commands include:

- An Fibre Channel port fails to move to the up state after such events as link failures, admin-up operations, or new connections.
- Unexpected link flaps.
- The port moves to error disabled state.

Obtain information about the module before these problems occur (if possible) and then obtain additional information after these problems occur.

Useful Commands at the FC-MAC Level

Troubleshooting a port problem involves analysis of the debug facilities provided by the FC-MAC driver, or the FC-MAC2 driver for the MDS 9120, MDS 9140, MDS 9216i, and the MPS-14/2 module. Table 8-2 lists several CLI debugging commands at the FC-MAC level.

Note: You must use the **attach module** CLI command to access these FC-MAC show commands.

Note: Use the **fcmac2** keyword for the MDS 9120, MDS 9140, MDS 9216i, and the MPS-14/2 module.

Table 8-2 Useful FC-MAC Port Commands

CLI Command	Description
show hardware internal fc-mac port *port* **link-status**	Performs a series of checks to isolate the problem.
show hardware internal fc-mac2 port *port* **link-status**	
show hardware internal fc-mac port *port* **port-info**	Provides the current state and configuration of the port.
show hardware internal fc-mac2 port *port* **port-info**	
show hardware internal fc-mac port *port* **statistics**	Gives all non-zero statistics for the port.
show hardware internal fc-mac2 port *port* **statistics**	
show hardware internal fc-mac port *port* **gbic-info**	Displays the current state of the SFP.
show hardware internal fc-mac2 port *port* **gbic-info**	

show hardware internal error	Collects interrupt statistics, error statistics, and exception log information for the entire module.
show hardware internal debug-info interface *fc-interface*	Represents an aggregation of a number of debug commands from all ASICs. The information includes interrupt-statistics, error-statistics, exception-log, link-events, and all debug information that is provided by the FC-MAC driver.

🖉**Note**: To enter CLI commands with the **internal** keyword, you must have an account that is a member of the network-admin group.

Isolating Port Issues Using the CLI

To isolate port issues using the CLI, follow these steps:

1. Use the **show interface** command to determine if the host HBA and the storage port can provide link level connectivity to their respective switches.

```
NPI1# show interface fc2/5 status
fc2/5 is down (Offline)


NPI2# show interface fc2/5 status
fc1/5 is up   Port mode is F
```

See Table 8-1 for details on nonoperational interface reasons.

2. If the port is down and offline, use the **no shutdown** command to bring the port online.

```
NPI1# config t
NPI1(config)# interface fc 2/5
NPI1(config-if)# no shutdown
```

3. Repeat Step 1 to determine if the port is online.

If either of the ports fails to remain in the online state, you might have a faulty GBIC, cabling or HBA/subsystem port.

4. If both ports are online, use the **show flogi** command to verify that the Fibre Channel ports for the host and storage have performed a fabric login (FLOGI) and are communicating with their respective switches.

Example 8-2 Using the show flogi Command

```
NPI1# sh flogi
     INTERFACE      VSAN  FCID        PORT NAME               NODE NAME
------------------- ---- -------- ----------------------- -----------------------
          fc2/5       1 0x7e0200 21:00:00:e0:8b:08:d3:20 20:00:00:e0:8b:08:d3:20
          fc2/7       1 0x7e0300 20:00:00:e0:69:41:98:93 10:00:00:e0:69:41:98:93
          fc2/11      1 0x7e0100 21:00:00:e0:8b:07:ca:39 20:00:00:e0:8b:07:ca:39
          fc2/14      1 0x7e0002 50:06:04:82:c3:a0:98:53 50:06:04:82:c3:a0:98:53
          fc8/31      1 0x7e0000 50:06:04:82:c3:a0:98:42 50:06:04:82:c3:a0:98:42


NPI2# sh flogi
```

```
     INTERFACE        VSAN    FCID        PORT NAME               NODE NAME
-------------------- ---- -------- ----------------------- -----------------------
        fc1/5           1 0x9f0100 50:06:04:82:c3:a0:98:5c 50:06:04:82:c3:a0:98:5c
        fc1/9           1 0x9f0020 21:00:00:e0:8b:08:dd:22 20:00:00:e0:8b:08:dd:22
        fc1/12          1 0x9f0040 50:06:04:82:c3:a0:98:52 50:06:04:82:c3:a0:98:52
        fc1/13          1 0x9f0300 21:00:00:e0:8b:08:a2:21 20:00:00:e0:8b:08:a2:21
        fc8/6           1 0x9f0101 20:00:00:e0:69:40:8d:63 10:00:00:e0:69:41:a0:12
        fc8/14          1 0x9f0003 50:06:04:82:c3:a0:98:4c 50:06:04:82:c3:a0:98:4c
```

5. If you do not see the ports in the **show flog**i output, use the **debug flogi even interface** command to isolate the FLOGI issue.

```
 NPI1# debug flogi event interface fc2/5
```

6. If the ports are in the **show flogi** output, use the **show fcns database** command to verify that the assigned FC ID during FLOGI exists in the name server database.

```
NPI2# show fcns database
-------------------------------------------------------------------------
FCID       TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
-------------------------------------------------------------------------
0x9f0100   N     50:06:04:82:c3:a0:98:5c (EMC)           scsi-fcp:target 250
0x7e0200   N     21:00:00:e0:8b:08:d3:20 (QLogic)        scsi-fcp:init
```

At this point, the HBA and subsystem ports have successfully established link-level connectivity and each one can communicate with its locally attached switch in the fabric. The next step is to verify zone membership. For a more detailed discussion and description about VSANs and zones see "Troubleshooting Zones and Zone Sets ".

Common Problems with Port Interfaces

The following issues are commonly seen with port interfaces:

- Port Remains in a Link Failure or Not Connected State
- Port Remains in Initializing State
- Unexpected Link Flapping Occurs
- Port Bounces Between Initializing and Offline States
- E Port Bounces Remains Isolated After a Zone Merge
- Port Cycles Through Up and Down States
- Port Is in ErrDisabled State
- Troubleshooting Fx Port Failure

Port Remains in a Link Failure or Not Connected State

If a link does not come up, the switch was unable to achieve bit or word synchronization with the node device. This situation may occur if nothing is connected to the interface, as in the case of a broken fiber, or if there is no bit synchronization between the switch interface and the directly connected Nx port. This problem might be the result of one or more of the possible causes listed in Table 8-3.

Symptom Port remains in a link-failure state.

Table 8-3 Port Remains in a Link-Failure State

Symptom	Possible Cause	Solution
Port remains in a link-failure state.	Port connection is bad.	Use the **show port internal info** CLI command to verify the port status is in link-failure. Use the **show hardware internal fc-mac port port gbic-info** CLI command to determine if there is a signal present. ✏️**Note**: You must use the **attach module** CLI command to access the FC-MAC show commands. Verify the type of media in use. Is it copper or optical, single-mode (SM) or multimode (MM)? Verify that the media is not broken or damaged. Is the LED on the switch green? Is the active LED on the host bus adapter (HBA) for the connected device on? Right-click the port in Device Manager and select **disable** and then **enable**, or use the **shut CLI** command followed by the **no shut** command to disable and enable the port. If this does not clear the problem, try moving the connection to a different port on the same or another module.
	There is no signal because of a transit fault in the SFP or the SFP may be faulty.	When this occurs, the port stays in a transit port state and you see no signal. There is no synchronization at the MAC level. The problem may be related to the port speed setting or autonegotiation. See the "Troubleshooting Port Problems" section. Verify that the SFP on the interface is seated properly. If reseating the SFP does not resolve the issue, replace the SFP or try another port on the switch.
	Link is stuck in initialization state or the link is in a point-to-point state.	Choose **Logs > Switch Resident > Syslog** on Device Manager or use the **show logging** CLI command to check for a Link Failure, Not Connected system message. Right-click the port in Device Manager and select **disable** and then **enable**, or use the **shut CLI** command followed by the **no shut** command to disable and enable the port. If this does not clear the problem, try moving the connection to a different port on the same or another module.

✏️**Note**: We recommend that you do not disable and then enable a T or TE port. This action affects all of the VSANs crossing the EISL instead of only the VSAN experiencing the problem.

Troubleshooting Port Problems

Start the debugging with the command **show hardware internal fc-mac port** *port* **link-status**. See the "Useful Commands at the FC-MAC Level" section to understand how to use the FC-MAC information.

Note: You must use the **attach module** CLI command to access the FC-MAC **show** commands.

When this command executes, it performs the following checks in the order shown here and displays the appropriate information:

1. Checks whether the port was declared a failure because of an exception. For additional information, use the **show process exceptionlog** CLI command.

2. Checks whether the port is administratively enabled.

3. Checks whether the physical link state is up. If the state is up, then it does the following:

- Checks for possible completion of the FLOGI process.

Note: FLOGI is transparent to the MAC driver and is based on some expected configuration. The MAC driver assumes that the FLOGI process is completed.

- Checks for error counters.

4. Checks whether the port is in the offline state. The port goes to the offline state if the FLOGI or ELP (in case of auto mode) on the port does not succeed.

5. Checks for pause state. A pause state is in an intermediate state (as maintained by the FC-MAC driver) after the link goes down and before the port is enabled by the Port Manager.

Note: The link reinitializes after a link down event is initiated only if enable is issued by the Port Manager.

---

6. Checks for the presence of SFP and GBIC. If present, FC-MAC checks for loss of signal. The loss of signal state indicates either the physical connectivity between two end ports is bad or there is a transmit fault in the SFP. Use the **show hardware internal fc-mac port** port **gbic-info** command to check for the transmit fault.

Note: You must use the **attach module** CLI command to access the FC-MAC show commands.

---

7. Checks for the speed and sync state of the port. If the port is in the speed initialization state, the following information is displayed:

- Auto speed is in progress is displayed if the port is in automode.
- Waiting for stable sync is displayed if the port is configured for a fixed speed.
- Sync not acquired is displayed if the MAC state indicates a loss of synchronization. In auto mode, this state is not necessarily an error. In any case, check the speed capabilities and configuration at both ends.

Port Remains in Initializing State

Symptom Port remains in the initializing state.

A port goes into the initialization state after a successful completion of link level initialization. For Fx and FL types of ports, the next step is to complete the FLOGI process. The port remains in the initialization state until the FLOGI (fabric login) process completes.

For E or TE port types, the next step is to complete the ELP process. If the ELP fails the port is moved to the offline state after a timeout and the entire process repeats until the port comes online.

Table 8-4 lists possible causes for FLOGI to fail for a given port and possible solutions.

Table 8-4 Port Remains in the Initializing State

Symptom	Possible Cause	Solution
Port remains in the initializing state.	The port is up because the link partner has put itself in a bypass mode.	Use the **show hardware internal fc-mac port** *port* **statistics** command to check whether the Class-3 input counter is increasing after the successful completion of link initialization. Note: You must use the **attach module** CLI command to access the FC-MAC **show** commands.
	The FLOGI packet was dropped somewhere in the data path, starting from FC-MAC to the FLOGI server.	Use the **show hardware internal fc-mac port** *port* **statistics** command to check for Class-3 packet counters. Note: You must use the **attach module** CLI command to access the FC-MAC **show** commands
	A software bug resulted in an error while handling the FLOGI packet.	Analyze the output of the **show hardware internal error** command for a possible drop of FLOGI packets somewhere in the path. We recommend that you do not disable and then enable a T or TE port. This would affect all the VSANs crossing the EISL instead of just the VSAN experiencing the problem. Right-click the port in Device Manager, and select **disable** and then **enable**, or use the **shut CLI** command followed by the **no shut** command to disable and enable the port. If this does not clear the problem, try moving the connection to a different port on the same or another module.

🖉**Note**: We recommend that you do not disable and then enable a T or TE port. This action affects all of the VSANs crossing the EISL instead of only the VSAN experiencing the problem.

Troubleshooting Port Registration Issues Using the CLI

To troubleshoot Nx port registration in the CLI, follow these steps:

1. Use the **show interface** *fc slot/port* command and verify that the Fibre Channel interface connected to the specified device is up and free of any errors. (See Example 8-3.)

Example 8-3 show interface Command Output

```
switch# show interface fc3/14
fc3/14 is up
    Hardware is Fibre Channel
    Port WWN is 20:8e:00:05:30:00:86:9e
    Admin port mode is FX
    Port mode is F, FCID is 0x780200 /* Operational State of the Port */
    Port vsan is 99    /* This is the vsan */
    Speed is 2 Gbps
    Receive B2B Credit is 16
    Receive data field size is 2112
    Beacon is turned off
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      1700 frames input, 106008 bytes, 0 discards
        0 CRC,  0 unknown class
        0 too long, 0 too short
      2904 frames output, 364744 bytes, 0 discards
      0 input OLS, 0 LRR, 0 NOS, 0 loop inits
      1 output OLS, 1 LRR, 0 NOS, 0 loop inits
```

If the interface is not working correctly, check the cabling and the host or storage device interface for faults. If the interface is working correctly, proceed to the next step.

2. Verify that the specified device appears in the FLOGI database. Enter the following command:

```
show flogi database vsan VSAN-ID
```

The system output might resemble:

```
switch# show flogi database vsan 99
--------------------------------------------------------------------------
INTERFACE  VSAN   FCID          PORT NAME            NODE NAME
--------------------------------------------------------------------------
fc3/14     99     0x780200  21:00:00:e0:8b:07:a4:36  20:00:00:e0:8b:07:a4:36
```

If the specified device appears in this output, skip to Step 7. If the device does not appear in the output, go to the next step.

3. Use the **shutdown** command in interface configuration mode to shut down the Fibre Channel interface connected to the specified device.

```
switch# config terminal
switch(config)# interface fcx/x
switch(config-if)# shutdown
```

🖉**Note**: We recommend that you do not disable and then enable a T or TE port. This action affects all of the VSANs crossing the EISL instead of only the VSAN experiencing the problem.

4. Use the **no shutdown** command on the Fibre Channel interface.

```
switch(config-if)# no shutdown
```

By shutting down the interface and bringing it back up, you can determine what happens when the connected device tries to log in to the interface.

Use the **show flogi internal event-history interface** command to view the events that occurred on the interface after you enabled it again. The comments that follow each section of output explain the meaning of the output.

🖉**Note**: To enter commands with the **internal** keyword, you must have an account that is a member of the network-admin group.

```
switch# show flogi internal event-history interface fc3/14
>>>>FSM: <[99]21:00:00:e0:8b:07:a4:36> has 9 logged transitions<<<<<
/* This is the [VSAN] followed by the pwwn of the N/NL port */


1) FSM:<[99]21:00:00:e0:8b:07:a4:36> Transition at 321686 usecs after Sun Feb 1
 04:18:15 1980
    Previous state: [FLOGI_ST_FLOGI_RECEIVED]
    Triggered event: [FLOGI_EV_VALID_FLOGI]
    Next state: [FLOGI_ST_GET_FCID]
/* The hba has sent an FLOGI to the switch */

2) FSM:<[99]21:00:00:e0:8b:07:a4:36> Transition at 322974 usecs after Sun Feb 1
 04:18:15 1980
    Previous state: [FLOGI_ST_GET_FCID]
    Triggered event: [FLOGI_EV_VALID_FCID]
    Next state: [FLOGI_ST_PERFORM_CONFIG]
/* Port Manager Obtains a valid FC_ID from the Domain Mgr */

3) FSM:<[99]21:00:00:e0:8b:07:a4:36> Transition at 323731 usecs after Sun Feb 1
 04:18:15 1980
    Previous state: [FLOGI_ST_PERFORM_CONFIG]
    Triggered event: [FLOGI_EV_CONFIG_DONE_PENDING]
    Next state: [FLOGI_ST_PERFORM_CONFIG]
/* ACLs are programmed and FIB {VSAN, FC_ID, portindex} is set */

4) FSM:<[99]21:00:00:e0:8b:07:a4:36> Transition at 323948 usecs after Sun Feb 1
 04:18:15 1980
    Previous state: [FLOGI_ST_PERFORM_CONFIG]
    Triggered event: [FLOGI_EV_LCP_RESPONSE]
    Next state: [FLOGI_ST_PERFORM_CONFIG]
/* LineCard responds that it is done */

5) FSM:<[99]21:00:00:e0:8b:07:a4:36> Transition at 325962 usecs after Sun Feb 1
 04:18:15 1980
    Previous state: [FLOGI_ST_PERFORM_CONFIG]
    Triggered event: [FLOGI_EV_NAME_SERVER_REG_RESPONSE]
    Next state: [FLOGI_ST_PERFORM_CONFIG]
/* Program the NameServer with wwn and FCID */

6) FSM:<[99]21:00:00:e0:8b:07:a4:36> Transition at 330381 usecs after Sun Feb 1
 04:18:15 1980
    Previous state: [FLOGI_ST_PERFORM_CONFIG]
```

```
   Triggered event: [FLOGI_EV_ZS_CFG_RESPONSE]
   Next state: [FLOGI_ST_PERFORM_CONFIG]
/* Response from ZoneServer */


7) FSM:<[99]21:00:00:e0:8b:07:a4:36> Transition at 331187 usecs after Sun Feb 1
 04:18:15 1980
   Previous state: [FLOGI_ST_PERFORM_CONFIG]
   Triggered event: [FLOGI_EV_RIB_RESPOSE]
   Next state: [FLOGI_ST_PERFORM_CONFIG]
/* Response from RIB */


8) FSM:<[99]21:00:00:e0:8b:07:a4:36> Transition at 331768 usecs after Sun Feb 1
 04:18:15 1980
   Previous state: [FLOGI_ST_PERFORM_CONFIG]
   Triggered event: [FLOGI_EV_ACL_CFG_RESPONSE]
   Next state: [FLOGI_ST_PERFORM_CONFIG]
/* Response from RIB */


9) FSM:<[99]21:00:00:e0:8b:07:a4:36> Transition at 331772 usecs after Sun Feb 1
 04:18:15 1980
   Previous state: [FLOGI_ST_PERFORM_CONFIG]
   Triggered event: [FLOGI_EV_CONFIG_DONE_COMPLETE]
   Next state: [FLOGI_ST_FLOGI_DONE]
/* Programming done */

   Curr state: [FLOGI_ST_FLOGI_DONE]
/* Flogi was successful */
```

If the device logs in successfully, proceed to the next step. Otherwise, you may have a problem with the device or its associated software.

5. Use the **shutdown** command in interface mode to shut down the Fibre Channel interface Then use the **no shutdown** command after turning on the debug as described in Step 6 and Step 7.

📝**Note**: We recommend that you do not disable and then enable a T or TE port. This action affects all the VSANs crossing the EISL instead of only the VSAN experiencing the problem.

---

6. Use the **debug fcns events register vsan** command to watch the FLOGI process take place.

```
 switch# debug fcns events register vsan 99Â
```

This command enables debug mode for name server registration. It generates messages on the switch console related to FCNS events. The system output resembles:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# interface fc3/14
switch(config-if)# no shutdown   /* enable the port */

switch(config-if)# Feb 17 04:42:54 fcns: vsan 99: Created entry for port-id 27800
Feb 17 04:42:54 fcns: vsan 99: Got Entry for port-id 27800
Feb 17 04:42:54 fcns: vsan 99: Registered port-name 36a4078be0000021 for port-id 780200
Feb 17 04:42:54 fcns: vsan 99: Registered node-name 36a4078be0000020 for port-id 780200
/* The wwpn and FCID for the port, note that the bytes in the world wide name are reversed
*/
Feb 17 04:42:54 fcns: vsan 99: Registered cos 8 for port-id 780200
/* Class of Service */

Feb 17 04:42:54 fcns: vsan 99: Registered port-type 1 for port-id 780200
/* Port Type */
```

```
Feb 17 04:42:54 fcns: vsan 99: Reading configuration for entry with port-name
36a4078be0000021, node-name 36a4078be0000020
Feb 17 04:42:54 fcns: vsan 99: No configuration present for this portname
Feb 17 04:42:54 fcns: vsan 99: No configuration present for this nodename
/* Port is now registered in nameserver, will send out RSCN to it */

Feb 17 04:42:54 fcns: vsan 99: Trying to send RSCN; affected port 780200
Feb 17 04:42:54 fcns: vsan 99: rscn timer started for port 780200
Feb 17 04:42:54 fcns: vsan 99: Saving new entry into pss
Feb 17 04:42:54 fcns: vsan 99: Sending sync message to the standby
Feb 17 04:42:54 fcns: vsan 99: sending accept response to 780200
/* RSCN was received by N/NL port */

Feb 17 04:42:54 fcns: vsan 99: sending accept response to fffc61
/* Other switch in fabric is notified */
Feb 17 04:42:55 fcns: vsan 99: rscn timer expired for port 780200
Feb 17 04:42:55 fcns: vsan 99: Saving modified entry into pss
Feb 17 04:42:55 fcns: vsan 99: Sending sync message to the standby

Feb 17 04:42:55 fcns: vsan 99: Registered fc4-types for port-id 780200
Feb 17 04:42:55 fcns: vsan 99: Registered fc4-features for fc4_type 8 for port-id 780200
/* FC4 Type, type 8 FCP has been registered */
```

Additional lines similar to these will be listed if more name server objects are registered.

7. If you are managing the switch over a Telnet connection, enable terminal monitoring by entering the **terminal monitor** command in exec mode.

The system output resembles:

```
switch# show fcns database detail vsan 99
-----------------------
VSAN:99    FCID:0x780200
-----------------------
port-wwn (vendor)    :21:00:00:e0:8b:07:a4:36 (QLogic) /* Port world wide name */
node-wwn             :20:00:00:e0:8b:07:a4:36
class                :3                       /* Fibrechannel class of service */
node-ip-addr         :0.0.0.0                 /* IP Address */
ipa                  :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init          /* Registered FC4 Types: example SCSI and
initiator */
symbolic-port-name   :
symbolic-node-name   :
port-type            :N                       /* Fibrechannel port type (F,FL) */
port-ip-addr         :0.0.0.0
fabric-port-wwn      :20:8e:00:05:30:00:86:9e /* wwn of the switch port */
hard-addr            :0x000000
```

Other attribute objects of the Nx port are registered one-per register operation after the FLOGI process is complete. The Nx port performs PLOGI to the well known WWN of the name server, 0xFFFFFC. The FC_CT Common Transport protocol uses Request and Accept messages to conduct transactions. To verify that additional attributes are correctly registered and recorded in the database, you can use the SAN-OS debug facility.

Note: The command **show fcns database detail vsan X** command displays a detailed list of all devices registered in the fabric.

Unexpected Link Flapping Occurs

Symptom Unexpected link flapping occurs.

When a port is flapping, it cycles through the following states, in this order, and then starts over again:

1. Initializing - The link is initializing.

2. Offline - The port is offline.

3. Link failure or not connected - The physical layer is not operational and there is no active device connection.

While troubleshooting unexpected link flapping, you need to know the following information:

- Who initiated the link flap.
- The actual link down reason.

Be sure to check the HBA, because a faulty HBA can produce symptoms on the attached switch port. For example, if an Nx port is self-diagnosed as faulty by the HBA driver or firmware, the driver can place the port in optical bypass mode. This situation results in the receive and transmit paths being internally connected through the port. If this happens, the switch port connected to the faulty device reaches bit and word synchronization with itself. If the port is configured in automode, the port issues an ELP and tries to initialize as an xE port, even if an end device is physically connected to that interface. In this case, a port reason code of isolation because of ELP failure can be displayed even if an ISL is not present.

Table 8-5 lists possible causes and solutions for link flapping.

Table 8-5 Unexpected Link Flapping Occurs

Symptom	Possible Cause	Solution
Unexpected link flapping occurs.	The bit rate exceeds the threshold and puts the port into an error disabled state.	Right-click the port in Device Manager and select **disable** and then **enable**, or use the **shut CLI** command followed by the **no shut** command to return the port to the normal state.
	The switch cannot complete the link reset. The link reset protocol failure results in a link flap that may be the result of: • The input buffer did not become empty within the link reset timeout period. • The link	The switch initiates the link reset when all credits are lost for more than four seconds or when there is a temporary signal or sync loss condition that lasts for less than 100 msec. See the "Troubleshooting Port Problems" section to verify this condition. Right-click the port in Device Manager and select **disable** and then **enable**, or use the **shut CLI** command followed by the **no shut** command to disable and enable the port. If this does not clear the problem, try moving the connection to a different port on the same or another module.

	partner did not respond to a link reset initiated by the switch.	
	There is a credit loss condition on an FL port.	When credit loss or a transmit stuck condition is detected in the FL port, the FC-MAC drive flaps the link as a recovery process. See the "Troubleshooting Port Problems" section.
	Some problem in the switch triggers the link flap action by the end device. Some of the causes are: • Packet drop in the switch, because of either a hardware failure or an intermittent hardware error such as X-bar sync loss. • Packet drop resulting from a software error. • A control frame is erroneously sent to the device.	Determine link flap reason as indicated by the MAC driver. Use the debug facilities on the end device to troubleshoot the problem. An external device may choose to reinitialize the link upon encountering the error. In such cases, the exact method of reinitializing the link varies by device. See the "Troubleshooting Port Problems" section for more information on externally triggered link flaps.

Note: We recommend that you do not disable and then enable a T or TE port. This action affects all the VSANs crossing the EISL instead of only VSAN experiencing the problem.

Link Initialization Flow

Fibre Channel primitive sequences establish and maintain a link, and they continue to be transmitted until a response has been received. Four primitive sequences are used in the link initialization process:

- Not operational sequence (NOS)
- Offline sequence (OLS)
- Link reset sequence (LRS)

- Link reset response sequence (LRR)

Figure 8-6 uses the ordered sets of 8b/10 encoding in the primary operational states. They include:

- AC = Active state
- LR = Link recovery state
- LF = Link failure state
- OF = Offline state

Figure 8-6 Link Initialization Flow
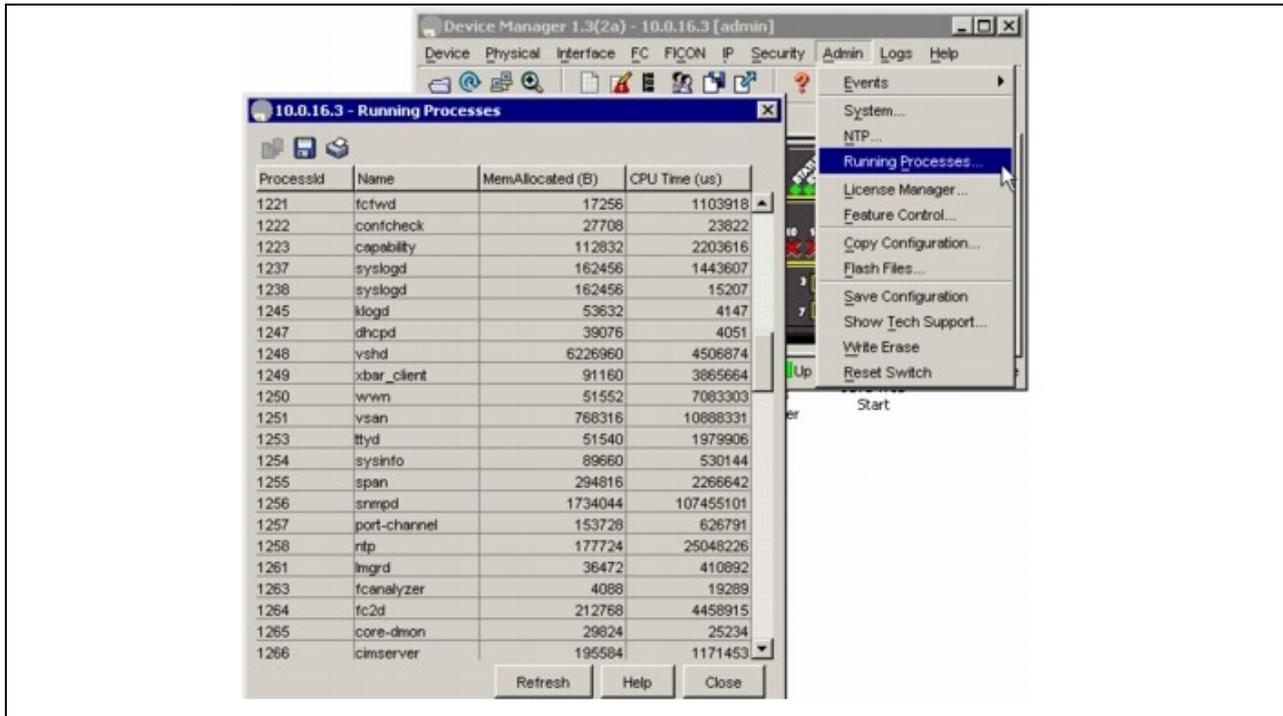
Figure 8-6 shows the link initialization flow. It displays the following ordered sets transmitted between the ports and the primary operational states of the port during the process:

1. Active state.

2. Link recovery state (LR):

     a. LR transmit substate (LR1)
     b. LR receive substate (LR2)
     c. LRR receive substate (LR3)

3. Offline state (OLS):

     a. OLS transmit substate (OL1)
     b. OLS receive substate (OL2)
     c. Wait for OLS substate (OL3)

4. Link failure state:

     a. NOS receive substate (LF1)
     b. NOS transmit substate (LF2)

The Cisco MDS 9000 Family switch maintains port counters for link initialization ordered sets, including OLS, LRR, and NOS for fabric connections, as well as primitives for arbitrated loop connections on FL ports and TL ports. Understanding the link initialization flow and viewing the port counters using **show interface** can be useful when you troubleshoot port initialization problems. Table 8-6 displays the reasons for a link flap.

Table 8-6 Link Flap Reasons Initiated by a Device Connected to the Switch

Reason	Description
Sync Loss	A synchronization loss condition persisted for more than 100 milliseconds. Look at the Invalid Transmission Word Count to check whether the physical link is really bad and if that caused the loss of synchronization. Sometimes this is not necessarily a problem with the physical link, but with the way some devices initialize the link. Use **attach module** to connect to the module and then use the **show hardware internal debug-info interface** CLI command. See Table 8-2.
Loss of signal	A signal loss condition persisted for more than 100 milliseconds. Look at the Invalid Transmission Word Count to check whether the physical link is really bad and if that caused the loss of synchronization. Sometimes this is not necessarily a problem with the physical link, but with the way some devices initialize the link. If the link does not come up after a flap, then probably the other end is in a shutdown state or the cable is broken. You can check for the broken or disconnected optical link by using the **show hardware internal fc-mac port** *port* **gbic-info** CLI command. **Note**: You must use the **attach module** CLI command to access the FC-MAC show commands
NOS received	An NOS received condition is detected. If the other end is an MDS port, then the NOS is transmitted by the other end in one of the following conditions: • A signal loss or sync loss condition is detected. • The port is administratively shut down. • The port is operationally down.
OLS received	An OLS received condition is detected.
LR received B2B	Link reset (LR) failed because of the receive queue (in the queue engine) not being empty.
Cr loss	Too many credit loss events occurred.
Rx queue overflow	The receive queue overflowed in the queue engine occurred. This can happen under the following conditions: • Improper credit configuration at one or both ends of the link. • A bad link can sometimes result in extra R_RDYs. Check for invalid transmission words at both ends.

LIP F* received	An loop initialization procedure (LIP) was received.
LC port shutdown	The port shutdown was invoked. Use the **show process exception** CLI command to check for any other errors.
LIP received B2B	An LIP was received while the Rx queue was not empty.
OPNy tmo B2B	An open circuit on a loop (OPNy) timeout occurred while the Rx queue was not empty.
OPNy Ret B2B	An OPNy was returned while the Rx queue was not empty.
Cr Loss B2B	Credit loss occurred while the Rx queue was not empty.

Viewing Port Counters

You can use the **show interface counters** command to view port counters. Typically, you only observe counters while actively troubleshooting, in which case you should first clear the counters to create a baseline. The values, even if they are high for certain counters, can be meaningless for a port that has been active for an extended period. Clearing the counters provides a better idea of the link behavior as you begin to troubleshoot.

Use one of the following commands in EXEC mode to clear all port counters or counters for specified interfaces:

- **clear counters interface all**
- **clear counters interface** *range*

The counters can identify synchronization problems by displaying a significant disparity between received and transmitted frames. For example, in the case of a broken fiber, if only the Tx path from the F port to the N port is broken, then the switch interface will still have an operational Rx path and will still obtain bit synchronization from the bit stream received from the N port. The switch port will also recognize an incoming NOS from the N port and reply with an OLS. However, because the transmitted OLS never reaches the N port, the R_T_TOV timer expires. In this scenario, the status of the port also shows Link failure or not connected.

The key difference between this case and the no bit synchronization case is that the input and output counts for OLS and NOS increment (as there is bit synchronization but no word synchronization). In this state, you can check that the Tx path from the switch to the Rx input on the N port interface is properly connected. A faulty transmitter on the switch's SFP or a faulty receiver on the N port's SFP could also cause the issue.

The output in Example 8-4 also displays evidence of corrupt data on the wire if there are a high number of CRCs and errors. Discards may or may not indicate a problem. For example, a frame can be discarded because of an ACL violation.

Example 8-4 show interface Command

```
mds# show interface fc4/2
fc4/2 is up
  . . .
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      322944 frames input, 19378384 bytes
        0 discards, 0 errors    <............................... Errors
        0 CRC,  0 unknown class
        0 too long, 0 too short
```

```
20439797 frames output, 41780390808 bytes
  0 discards, 0 errors
0 input OLS, 0 LRR, 0 NOS, 0 loop inits
2 output OLS, 2 LRR, 0 NOS, 0 loop inits <................Link Initialization
12 receive B2B credit remaining
1 transmit B2B credit remaining
```

Port Bounces Between Initializing and Offline States

Symptom Port bounces between the initializing and offline states.

An ELP failure may result in a port bouncing between the initializing and offline states. Table 8-7 lists possible causes and solutions to this problem.

Table 8-7 Port Bounces Between the Initializing and Offline States

Symptom	Possible Cause	Solution
Port bounces between the initializing and offline states.	An ELP packet was dropped in one of the two switches.	Use the **show hardware internal fc-mac port** *port* **statistics** CLI command and the **show hardware internal error** command. Analyze the output of the two commands for possible packet drops. See the "Troubleshooting ELP Issues Using the CLI" section. See also the "E Port Is Isolated in a VSAN" section. Note: You must use the **attach module** CLI command to access the FC-MAC **show** commands
	There is a software bug or incompatibility in handling the ELP process.	Analyze the event history provided by the Port Manager after using the **show port internal event-history** CLI command. See the "Troubleshooting ELP Issues Using the CLI" section.

Troubleshooting ELP Issues Using the CLI

To troubleshoot ELP issues using the CLI, follow these steps:

1. Use the **show interface** command to verify E port isolation**:**

```
switch# show interface fc2/4
```

```
fc2/4 is down (Isolation due to ELP failure)
    Hardware is Fibre Channel, WWN is 20:44:00:05:30:00:18:a2
    vsan is 1
    Beacon is turned off
    1445517676 packets input, 727667035658 bytes, 0 discards
    0 input errors, 0 CRC, 0 invalid transmission words
        0 address id, 0 delimiter
    Received 0 runts, 0 jabber, 0 too long, 0 too short
        0 EOF abort, 0 fragmented, 0 unknown class
        100 OLS, 67 LRR, 37 NOS, 0 loop inits
    133283352 packets output, 1332969530 bytes
    Transmitted 198 OLS, 50 LRR, 0 NOS, 10 loop inits
```

In this example, the interface indicates a link isolation caused by an ELP failure on an E port. The ELP is a frame sent between two switches to negotiate fabric parameters.

2. Verify that the following parameters match on each switch in the VSAN using the **show fctimer** command:

- ED_TOV timer
- RA_TOV timer
- FS_TOV timer

Note: Because fabric parameters are configured on a per-VSAN basis, they are required to be the same for all switches within a VSAN.

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

This sample output shows the default settings for these timeout values.

3. Use the **fctimer** command in config mode to globally set these timeout values across all VSANs or use the **fctimer D_S_TOV** *timeout* **vsan** *vsan-id* command, to set the D_S_TOV timeout for a particular VSAN to override the global values.

4. Use the **show port internal info interface fc** command to verify that Rx buffer size matches on both ends of the ISL.

Note: To enter commands with the **internal** keyword, you must have an account that is a member of the network-admin group.

```
switch# show port internal info interface fc2/1
fc2/1 - if_index:  1080000
  Admin Config - state(up), mode(Auto), speed(auto), trunk(no trunk)
    beacon(off), snmp trap(on), tem(false)
    bb_credit(default), rxbufsize(2112), encap(default)
    description()
  Operational Info - state(down), mode(ALL), speed(auto), trunk(no trunk)
    state reason(Link failure or not-connected)
    phy port enable (1), phy layer (FC)
    participating(1), port_vsan(1), null_vsan(0), fcid(0x000000)
    current state [PI_FSM_ST_LINK_INIT]
    port_init_eval_flag(0x00000001), cfg wait for none
    Mts node id 0x202
    cnt_link_failure(0), cnt_link_success(0), cnt_port_up(0)
```

Troubleshooting ELP Issues Using the CLI   27

```
   cnt_cfg_wait_timeout(0), cnt_port_cfg_failure(0), cnt_init_retry(0)
 Port Capabilities -
   Modes: E,TE,F,FL,TL,SD
   Min Speed: 1000
   Max Speed: 2000
   Max Tx Bytes: 2112
   Max Rx Bytes: 2112
   Max Tx Buffer Credit: 255
   Max Rx Buffer Credit: 16
   Max Private Devices: 63
   Max Sourcable Pkt Size: 2112
   Hw Capabilities: 0xb
   Connector Type: 0x0
 SFP info -
   Min Speed: 1000
   Max Speed: 2000
   Module Type: 8
   Connector Type: 7
   Gigabit Eth Compliance Codes: 0
   FC Transmitter Type: 3
   Vendor Name: PICOLIGHT
   Vendor ID: 0:4:133
   Vendor Part Num: PL-XPL-00-S23-28
   Vendor Revision Level:
 Trunk Info -
   trunk vsans (allowed active) (1)
```

E Port Bounces Remains Isolated After a Zone Merge

Symptom E port remains isolated after a zone merge.

An E port may be isolated because of a zone merge failure. Table 8-8 lists possible causes and solutions to this problem.

Table 8-8 E Port Remains Isolated after a Zone Merge

Symptom	Possible Cause	Solution
E port remains isolated after a zone merge.	The active zone sets on the two switches differ from each other in terms of zone membership (provided there are zones at either side with identical names).	See the "Troubleshooting E port Isolation using Fabric Manager" section or the "Troubleshooting E port Isolation using Fabric Manager" section.
	The active zone set on both switches contains a zone with the same name but with different zone members.	

Troubleshooting E Port Isolation Using Fabric Manager

To troubleshoot E port isolation due to zoning using Fabric Manager, follow these steps:

1. Choose **Switches > Interfaces > FC Physical** to verify that the E port did not come up because of a zone merge failure.

Note: Zoning information exists on a per-VSAN basis. Therefore, for a TE port, it may be necessary to verify that the zoning information does not conflict for any allowed VSAN.

2. Choose **Zone > Edit Local Full Zone Database** to verify the zoning configuration.

3. Use one of the following two approaches to resolve a zone merge failure:

- Choose **File > Restore** from the Edit Local Full Zone Database dialog box to overwrite the zoning configuration of one switch with the other switch's configuration.

  The **Restore** option overwrites the local switch's active zone set with that of the remote switch.

- If the zoning databases between the two switches are overwritten, you cannot use the **Restore** option. To work around this, you can manually change the content of the zone database on either of the switches using the Edit Local Full Zone Database, and then choose **Switches > Interfaces > FC Physical** and select **down** and then **up** on the Admin Status drop-down menu for the isolated port.

4. If the isolation is specific to one VSAN and not on an E port, the correct way to issue the cycle up or down is to remove the VSAN from the list of allowed VSANs on that trunk port, and reinsert it.

  a. Choose **Switches > Interfaces > FC Physical** and click the **Trunk Config** tab.
  b. Remove the VSAN from the Allowed VSAN list and click **Apply Changes.**
  c. Add the VSAN back to Allowed VSAN list and click **Apply Changes.**

Note: We recommend that you do not disable and then enable a T or TE port. This action can affect all of the VSANs crossing the EISL, instead of only the VSAN experiencing the isolation problem.

By using the Zone Merge Analysis tool in Fabric Manager, you can check the compatibility of two active zone sets in two switches before actually merging the two zone sets. Refer to the *Cisco MDS 9000 Fabric Manager Configuration Guide* for more information.

Troubleshooting E Port Isolation Using the CLI

To troubleshoot E port isolation due to zoning using the CLI, follow these steps:

1. Use the **show interface** command output to verify that the E port did not come up because of a zone merge failure.

Note: Zoning information exists on a per-VSAN basis. Therefore, for a TE port, you might nees to verify that the zoning information does not conflict for any allowed VSAN.

```
switch# show interface fc2/14

fc2/14 is down (Isolation due to zone merge failure)
    Hardware is Fibre Channel, WWN is 20:4e:00:05:30:00:63:9e
    vsan is 1
    Beacon is turned off
      40 frames input, 1056 bytes, 0 discards
      0 runts, 0 jabber, 0 too long, 0 too short
      0 input errors, 0 CRC, 3 invalid transmission words
      0 address id, 0 delimiter
      0 EOF abort, 0 fragmented, 0 unknown class
```

```
79 frames output, 1234 bytes, 16777216 discards
Received 23 OLS, 14 LRR, 13 NOS, 39 loop inits
Transmitted 50 OLS, 16 LRR, 21 NOS, 25 loop inits
```

2. Verify the zoning information using the following commands:

- **show zone vsan** *vsan-id*
- **show zoneset vsan** *vsan-id*

3. Use one of the following two approaches to resolve a zone merge failure:

- Overwrite the zoning configuration of one switch with the other switch's configuration. This can be done with the following commands:
  - ♦ **zone copy interface fc** *slot*/*port* **import vsan** *vsan-id*
  - ♦ **zone copy interface fc s***lot*/*port* **export vsan** *vsan-id*

  The **import** option of the command of overwrites the local switch's active zoneset with that of the remote switch. The **export** option overwrites the remote switch's active zoneset with the local switch's active zone set.

- If the zoning databases between the two switches are overwritten, you cannot use the **import** option. To work around this, you can manually change the content of the zone database on either of the switches, and then use a **shutdown** and **no shutdown** command sequence on the isolated port.

4. If the isolation is specific to one VSAN and not on an E port, the correct way to issue the cycle up or down is to remove the VSAN from the list of allowed VSANs on that trunk port, and reinsert it.

Note: We recommend that you do not disable and then enable a T or TE port. This action can affect all the VSANs crossing the EISL, instead of only the VSAN experiencing the isolation problem.

Port Cycles Through Up and Down States

Symptom Port cycles through the up and down states.

This problem may be attributable to an error experienced by the connected device. Table 8-9 lists the possible causes and solutions for this problem.

Table 8-9 Port Cycles Through the Up and Down States

Symptom	Possible Causes	Solutions
Port cycles through the up and down states.	One or more packets were dropped in the switch.	Analyze the debug log provided by the Nx port. Select **Tools > Traceroute** using Fabric Manager or use the **fctrace** CLI command to analyze the link.
	There is a problem in FLOGI processing.	Look for FLOGI messages in the logs for this port. See the "Troubleshooting Port Registration Issues Using the CLI" section
	The device received	

	unexpected packets.	
	There was a higher layer software error.	

Port Is in ErrDisabled State

The ErrDisabled state indicates that the switch detected a problem with the port and disabled the port. This state could be caused by a flapping port or a high number of bad frames (CRC errors), potentially indicating something is wrong with the media.

Symptom Port is in ErrDisabled state.

An E port may be isolated because of a zone merge failure. Table 8-10 lists possible causes and solutions to this problem.

Table 8-10 Port is in ErrDisabled State

Symptom	Possible Cause	Solution
Port is in ErrDisabled state.	Flapping port.	See the "Verifying the ErrDisable State Using the CLI" section. Verify the SFP, cable, and connections.
	Switch detected a high amount of bad frames (CRC errors), potentially indicating something wrong with the media.	

Verifying the ErrDisable State Using the CLI

To resolve the ErrDisable state using the CLI, follow these steps:

1. Use the **show interface** command to verify that the switch detected a problem and disabled the port. Check cables, SFPs, and optics.

```
mds# show interface fc1/14
fc1/14 is down (errDisabled)
```

2. Use the **show port internal event-history interface** command to view information about the internal state transitions of the port. In this example, port fc1/7 entered the ErrDisabled state because of a capability mismatch, or CAP MISMATCH. You might not know how to interpret this event, but you can look for more information with other commands.

```
mds# show port internal event-history interface fc1/7

>>>>FSM: <fc1/7> has 86 logged transitions<<<<

1) FSM:<fc1/7> Transition at 647054 usecs after Tue Jan  1 22:44..
    Previous state: [PI_FSM_ST_IF_NOT_INIT]
    Triggered event: [PI_FSM_EV_MODULE_INIT_DONE]
    Next state: [PI_FSM_ST_IF_INIT_EVAL]
```

```
2) FSM:<fc1/7> Transition at 647114 usecs after Tue Jan  1 22:43..
   Previous state: [PI_FSM_ST_IF_INIT_EVAL]
   Triggered event: [PI_FSM_EV_IE_ERR_DISABLED_CAP_MISMATCH]
   Next state: [PI_FSM_ST_IF_DOWN_STATE]
```

3. Use the **show logging logfile** command to display the switch log file and view a list of port state changes. In this example, an error was recorded when someone attempted to add port fc1/7 to PortChannel 3. The port was not configured identically to PortChannel 3, so the attempt failed.

```
mds# show logging logfile
 . . .
Jan  4 06:54:04 switch %PORT_CHANNEL-5-CREATED: port-channel 17 created

Jan  4 06:54:24 switch %PORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-channel
17 is down (No operational members)

Jan  4 06:54:40 switch %PORT_CHANNEL-5-PORT_ADDED: fc1/8 added to port-channel 7

Jan  4 06:54:56 switch %PORT-5-IF_DOWN_ADMIN_DOWN: Interface fc1/7 is down
(Admnistratively down)

Jan  4 06:54:59 switch %PORT_CHANNEL-3-COMPAT_CHECK_FAILURE: speed is not compatible

Jan 4 06:55:56 switch%PORT_CHANNEL-5-PORT_ADDED: fc1/7 added to port-channel 7
```

Troubleshooting Fx Port Failure

Fx port problems can be caused by a variety of configuration issues. While most issues can be solved by simply ensuring that the ports are configured properly, some issues require the use of more in-depth troubleshooting techniques.

Overview of Symptoms

An F port might be connected to a single N port, which is the mode used by peripheral devices (hosts or storage). In case all of the possible cases you can encounter in troubleshooting an Fx port, two different scenarios can occur:

- The port does not come up (check the interface configuration, cabling, and the port connected to the switch).
- The port comes up, but the host cannot communicate with the storage subsystem (check the VSAN and zone configurations).

Typical end-user questions that lead to Fx port troubleshooting include:

- Why is no storage visible on my newly installed server?
- Why is previously assigned storage not visible to my server after reboot?

Typical administrator questions to investigate:

- Why does the server fail to complete FLOGI to the switch?
- Why does the storage device fail to complete FLOGI to the switch?

Figure 8-7 illustrates one possible method for troubleshooting Fx ports.

Figure 8-7 Fx Port Troubleshooting Method

Verifying the ErrDisable State Using the CLI   32
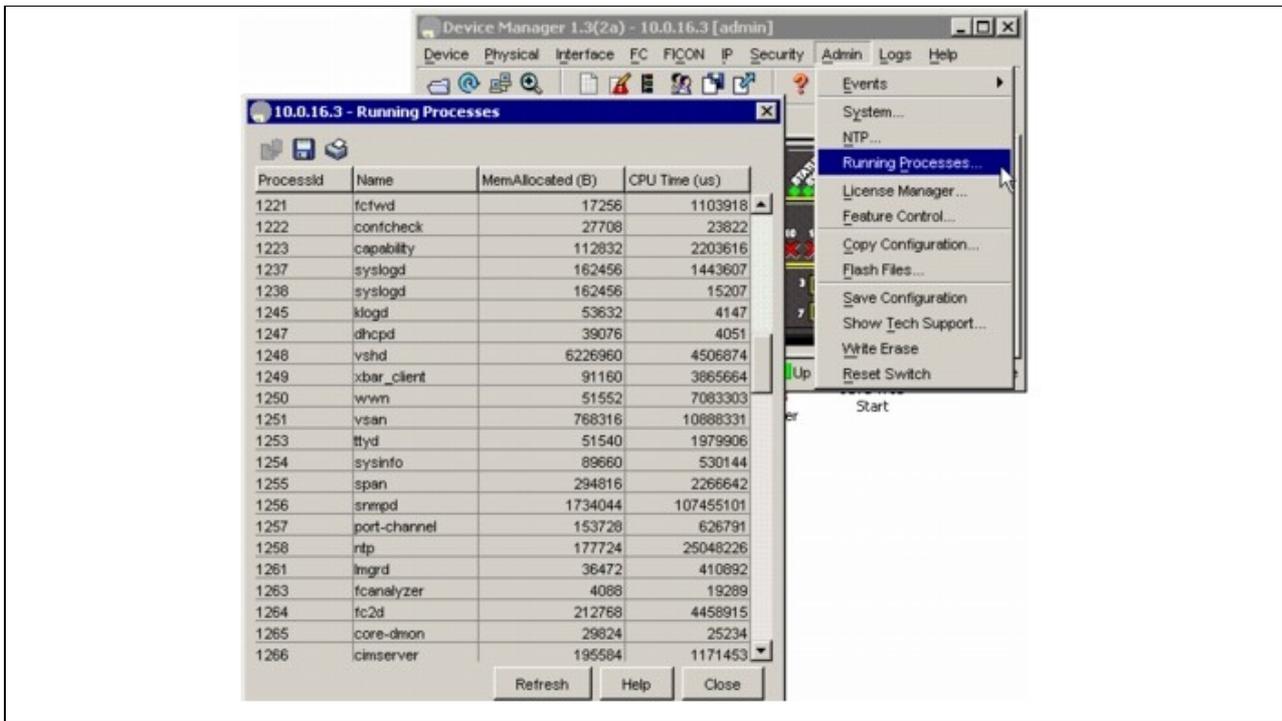
Back to Main Page: Cisco MDS SAN-OS Troubleshooting Guide