CHAPTER 3

Troubleshooting

This chapter describes these topics for troubleshooting problems:

- Diagnosing Problems, page 3-1
- Clearing the Switch Module IP Address and Configuration, page 3-5
- Replacing a Failed Stack Member, page 3-5
- Locating the Switch Module Serial Number, page 3-6

Diagnosing Problems

The LEDs on the switch module front panel provide troubleshooting information. They show power-on self-test (POST) failures, port-connectivity problems, and overall switch module performance. You can also get statistics from the CLI or from an SNMP workstation. See the software configuration guide and the switch command reference on Cisco.com or the documentation that came with your SNMP application for more information.

This section includes these troubleshooting topics:

- Verify the Switch Module POST Results, page 3-1
- Look at the Switch Module LEDs, page 3-2
- Confirm the Switch Module Connections, page 3-2
- Verify the Switch Module Performance, page 3-4

Verify the Switch Module POST Results

As the switch module powers on, it begins the POST, a series of tests that runs automatically to ensure that the switch functions properly. It might take several minutes for the switch to complete POST.

When the switch begins POST, the system LED slowly blinks green. When POST completes, the system LED blinks amber. If POST fails, the system LED remains amber. If POST completes successfully, the system LED rapidly blinks green.

Note POST failures are usually fatal. Contact your Cisco technical support representative if your switch does not pass POST.

Look at the Switch Module LEDs

You must have physical access to the switch module to do this. Look at the port LEDs for troubleshooting information about the switch module. See the "LEDs" section on page 1-5 for a description of the LED colors and their meanings.

Confirm the Switch Module Connections

Review this section when troubleshooting switch module connectivity problems.

Bad or Damaged Cable

Always test the cable for marginal damage or failure. A cable might be sufficient to connect at the physical layer but then cause packet corruption because of subtle damage to its wiring or connectors. You can identify this situation because the port will have many packet errors, or the port will constantly lose and regain link. In these situations:

- Exchange the copper or fiber-optic cable with a known, good cable.
- Look for broken or missing pins on cable connectors.
- Rule out any insufficient patch panel connections or media convertors between the source and the destination. If possible, bypass the patch panel or eliminate faulty media convertors, such as fiber-optic-to-copper convertors.
- Try using the cable in another port or interface to see if the problem also exists there.

Ethernet and Fiber Cables

Make sure that you have the correct cable type for the connection:

- For Ethernet, use Category 3 copper cable for 10 Mb/s unshielded twisted pair (UTP) connections. Use either Category 5, Category 5e, or Category 6 UTP for 10/100 or 10/100/1000 Mb/s connections.
- For fiber-optic connectors, verify that you have the correct cable for the distance and port type. Make sure that the ports on the connected device match and that they use the same type of encoding, optical frequency, and fiber type. For more information about cabling, see Appendix B, "Connector and Cable Specifications."
- For copper connections, determine if a crossover cable was used when a straight-through cable was required, or the reverse. Enable auto-MDIX on the switch module, or replace the cable.

Link Status

Verify that both sides have link. A single broken wire or one shutdown port can cause one side to show link, but the other side does not have link.

A link LED does not guarantee that the cable is fully functional. The cable might have encountered physical stress that causes it to function at a marginal level. If the link light for the port does not come on:

- Connect the cable from the switch module to a known, good device.
- Make sure that both ends of the cable are connected to the correct ports.
- Verify that both devices have power.

- Verify that you are using the correct cable type. See Appendix B, “Connector and Cable Specifications,” for more information.
- Test for loose connections. Sometimes a cable appears to be seated, but is not. Disconnect and then reconnect the cable.

SFP Module Port Issues

Use only Cisco small form-factor pluggable (SFP) modules on the switch module. Each Cisco module has an internal serial EEPROM that is encoded with security information. This encoding provides a way for Cisco to identify and validate that the module meets the requirements for the switch module. Test these items:

- Bad or wrong SFP module. Exchange the suspect module with a known, good module. Verify that this module supports this platform. See the “Cisco TwinGig Converter Module” section on page 1-4 for a list of supported SFP modules.
- Use the **show interfaces** privileged EXEC command to determine the port or module error-disabled, disabled, or shutdown status. Re-enable the port if necessary.
- Make sure that all fiber-optic connections are properly cleaned and securely connected.

Port and Interface Settings

Verify that the port or interface is not disabled or for some reason powered down. If a port or interface is manually shut down on one or the other side of the link, the link does not come up until you re-enable the port. Use the **show interfaces** privileged EXEC command to determine the port or interface error-disabled, disabled, or shutdown status on both sides of the connection. If necessary, re-enable the port or the interface.

Ping the End Device

Test the end device by pinging it from the directly connected switch module first, and then work your way back port by port, interface by interface, trunk by trunk, until you find the source of the connectivity issue. Make sure that each switch module can identify the end device MAC address in its Content-Addressable Memory (CAM) table.

Spanning Tree Loops

Spanning Tree Protocol (STP) loops can cause serious performance issues that might appear to be port or interface problems. In this situation, the switch module bandwidth is used repeatedly by the same frames, crowding out legitimate traffic.

A unidirectional link can cause loops. This occurs when the traffic that the switch module sends is received by its neighbor, but the switch module does not receive the traffic that is sent from the neighbor. A broken fiber-optic cable, other cabling, or a port issue could cause this one-way communication.

You can enable the UniDirectional Link Detection (UDLD) protocol on the switch module to help identify difficult-to-find unidirectional link problems. UDLD supports a normal mode of operation (the default) and an aggressive mode. In normal mode, UDLD detects unidirectional links because of incorrectly connected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links caused by one-way traffic on fiber-optic and twisted-pair links and by incorrectly connected interfaces on fiber-optic links. For information about enabling UDLD on the switch module, see the “Understanding UDLD” section in the software configuration guide.

Verify the Switch Module Performance

Review this section when you troubleshoot switch module performance problems.

Speed, Duplex, and Autonegotiation

If the port statistics show a large number of alignment errors, frame check sequence (FCS), or late-collisions errors, a speed or duplex mismatch might be the problem.

A common issue with speed and duplex occurs when the duplex settings are mismatched between two switches, between a switch module and a router, or between the switch module and a workstation or server. This can happen when you manually set the speed and duplex or because of autonegotiation issues between the two devices.

These circumstances can result in a mismatch:

- A manually set speed or duplex parameter is different from the manually set speed or duplex parameter on the connected port.
- A port is set to autonegotiate, and the connected port is set to full duplex with no autonegotiation.

To maximize switch module performance and ensure a link, follow one of these guidelines when you set or change the settings for duplex and speed:

- Let both ports autonegotiate both speed and duplex.
- Manually set the speed and duplex parameters for the ports on both ends of the connection.
- If a remote device does not autonegotiate, configure the duplex settings on the two ports to match. The speed parameter can adjust itself even if the connected port does not autonegotiate.

Autonegotiation and Network-Interface Cards

Problems sometimes occur between the switch module and third-party network-interface cards (NICs). By default, the switch module ports and interfaces are set to autonegotiate. It is common for devices such as laptop computers or other devices to also be set to autonegotiate, yet sometimes autonegotiation issues occur.

To troubleshoot autonegotiation problems, try manually setting both sides of the connection. If this does not solve the problem, the firmware or software on your NIC might be causing the problem. Upgrade the NIC driver to the latest version available from the manufacturer.

Cabling Distance

If the port statistics show excessive FCS, late-collision, or alignment errors, verify that the cable distance from the switch module to the connected device meets the recommended guidelines. See the "Cable and Adapter Specifications" section on page B-4 for cabling guidelines.

Clearing the Switch Module IP Address and Configuration

This section describes how to reset the switch module by rerunning the initial configuration dialog (system configuration dialog). These are reasons why you might want to reset the switch module:

- You installed the switch module in your network and cannot connect to it because you assigned the wrong IP address.
- You want to clear all the configuration settings from the switch module and assign a new IP address.

Caution This procedure clears the IP address and all configuration information stored on the switch module. Do not follow this procedure unless you want to completely reconfigure the switch module.

To reset the switch module:

1. At the switch module prompt, enter **enable**, and press **Return** or **Enter**.
2. At the Privileged EXEC prompt, switch module#, enter setup and press **Return** or **Enter**.

The switch module displays the prompt to run the initial configuration dialog. The switch module now behaves like an unconfigured switch module. You can configure the switch module by using the CLI setup procedure described in Appendix C, "Configuring the Switch with the CLI-Based Setup Program"

Replacing a Failed Stack Member

If you need to replace a failed stack member, you can hot swap or replace the switch module by following this procedure:

1. Get a replacement switch module that has the same model number as the failed switch module.
2. Power down the failed switch module through the Onboard Administrator.
3. Install the replacement switch module in the server chassis.

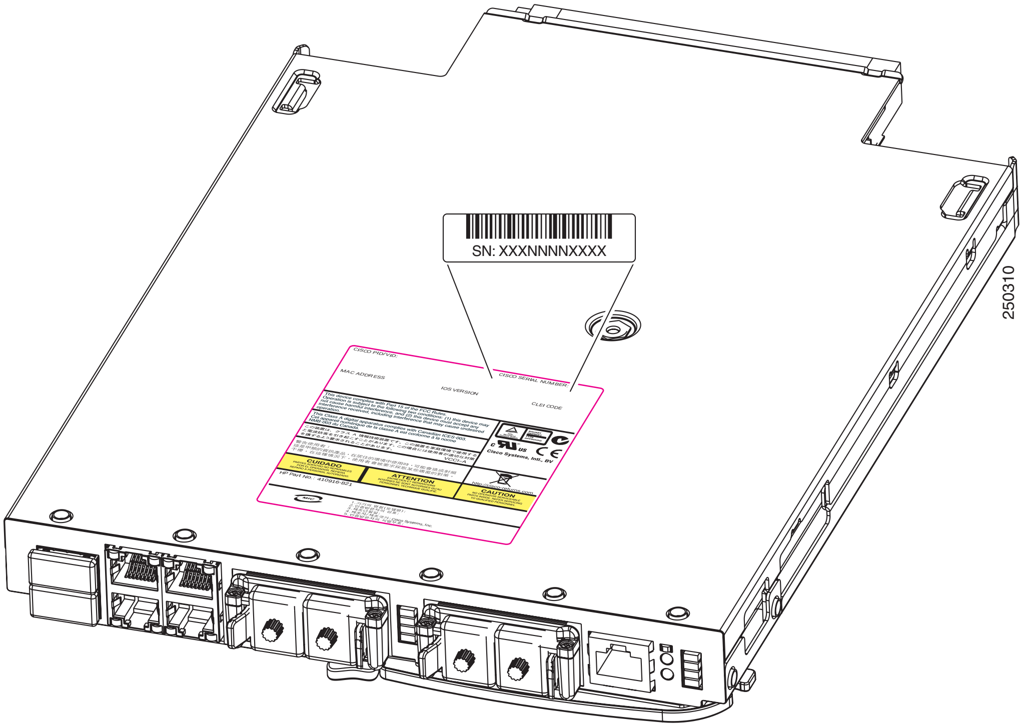
   If you manually set the member numbers for any members in the stack, you need to manually assign the replacement switch module with the same member number as the failed switch module.
   To manually assign the member number, install the replacement switch module, and wait for it to boot up. Use the CLI to manually assign the member number (see the software configuration guide for instructions) before you connect the switch module to the stack.
4. Connect the switch to the stack.
5. Make the same Gigabit Ethernet connections on the replacement switch module that were on the failed switch module.
6. Reinstall any transceiver modules and cable connections.
7. Power on the replacement switch through the Onboard Administrator.

The replacement switch module will have the same configuration for all the interfaces as the failed switch module and will function the same as the failed switch module.

Locating the Switch Module Serial Number

If you contact Cisco Technical Assistance, you need to know the serial number of your switch module. Figure 3-1 shows the serial number location on your switch module. You can also use the **show version** command to get the serial number.

Figure 3-1 Serial Number Location


SN: XXXNNNNXXXX
250310