CHAPTER 4

Troubleshooting

Diagnosing Problems

The LEDs on the front panel provide troubleshooting information about the switch. They show power-on self-test (POST) failures, port-connectivity problems, and overall switch 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.

Switch POST Results

As the switch 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 blinks green, and the other LEDs remain solid green. When POST succeeds, the System LED becomes solid green. The other LEDs turn off and return to their operating status. If the switch fails POST, the System LED is solid amber.

You can use the **show diagnostics post** user EXEC command to display the POST results.

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

Switch LEDs

You must have physical access to the switch to do this. Look at the port LEDs for troubleshooting information about the switch. See the "LEDs" section on page 1-7 for a description of the LED colors and their meanings.

Switch Connections

Bad or Damaged Cable

Always examine the cable for marginal damage or failure. A cable might be just good enough to connect at the physical layer, but it could corrupt packets as a result of subtle damage to the wiring or connectors. You can identify this situation because the port has many packet errors or the port constantly flaps (loses and regains link).

- Examine or exchange the copper or fiber-optic cable with a known, good cable.
- Look for broken or missing pins on cable connectors.
- Rule out any bad patch panel connections or media convertors between the source and the destination. If possible, bypass the patch panel, or eliminate faulty media convertors (fiber-optic-to-copper).
- Try the cable in another port or interface, if possible, to see if the problem follows the cable.

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 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 connected device ports both match and use the same type encoding, optical frequency, and fiber type.
- For copper connections, determine if a crossover cable was used when a straight-through was required or the reverse. Enable auto-MDIX on the switch, or replace the cable. See Table 2-1 for recommended Ethernet cables.

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 port 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 port LED does not turn on:

- Connect the cable from the switch 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.
- Look for loose connections. Sometimes a cable appears to be seated, but is not. Disconnect the cable and then reconnect it.

SFP Module Port Issues

Use only Cisco SFP modules on the switch. 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. Check these items:

- Bad or wrong SFP module. Exchange the suspect module with known good module. Verify that the module is supported on this platform. (The switch release notes on Cisco.com list the SFP modules that the switch supports.)
- Use the **show interfaces** privileged EXEC command to see if the port or module is error-disabled, disabled, or shutdown. Re-enable the port if needed.
- Make sure that all fiber connections are properly cleaned and securely connected.

Port and Interface Settings

An obvious but sometimes overlooked cause of port connectivity failure is a disabled interface. Verify that the interface is not disabled or powered off for some reason. If an interface is manually shut down on one side of the link or the other side, the link does not come up until you re-enable the interface. Use the **show interfaces** privileged EXEC command to see if the interface is error-disabled, disabled, or shutdown on either side of the connection. If needed, re-enable the interface.

Ping the End Device

Ping from the directly connected switch 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 can identify the end device MAC address in its Content-Addressable Memory (CAM) table.

Spanning Tree Loops

STP loops can cause serious performance issues that look like port or interface problems.

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

The UniDirectional Link Detection (UDLD) protocol helps identify unidirectional link problems. For more information, see the "Understanding UDLD" section in the switch software configuration guide on Cisco.com.

Switch Performance

Speed, Duplex, and Autonegotiation

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

A common issue with speed and duplex is when the duplex settings are mismatched between two switches, between a switch and a router, or between the switch and a workstation or server. Mismatches can happen when manually setting the speed and duplex or from autonegotiation issues between the two devices.

To maximize switch performance and to ensure a link, follow one of these guidelines when changing the duplex or speed settings.

- 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, set the same duplex settings on the two ports. The speed parameter adjusts itself even if the connected port does not autonegotiate.

Autonegotiation and NICs

Problems sometimes occur between the switch and third-party network interface cards (NICs). By default, the switch ports and interfaces are set to autonegotiate. Devices like laptops or other devices are commonly set to autonegotiate, yet sometimes autonegotation issues occur.

To troubleshoot autonegotiation problems, try manually setting both sides of the connection. If this does not solve the problem, there could be a problem with the firmware or software on your NIC. You can resolve this by upgrading the NIC driver to the latest available version.

Cabling Distance

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

Clearing the Switch IP Address and Configuration

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

- You installed the switch 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 and assign a new IP address.

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

To reset the switch:

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

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

Finding the Switch Serial Number

If you contact Cisco Technical Assistance, you need to know the serial number of your switch. Use these figures to locate the serial number location. You can also use the **show version** privileged EXEC command or the **show inventory** user EXEC command to get the serial number.

Figure 4-1 Serial Number Location on the Cisco ME 3400E-24TS-M

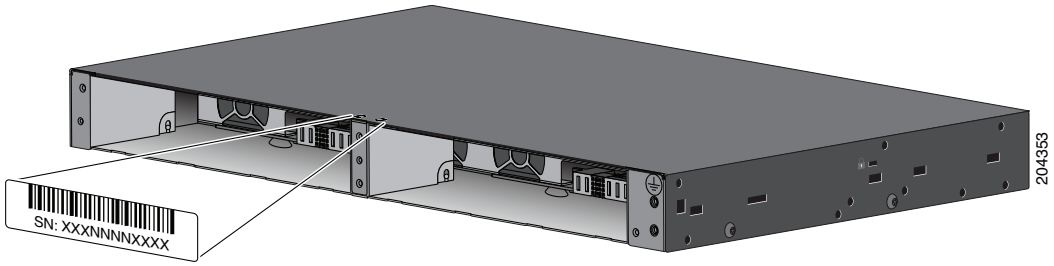

Figure 4-2 Serial Number Location on the Cisco ME 3400EG-12CS

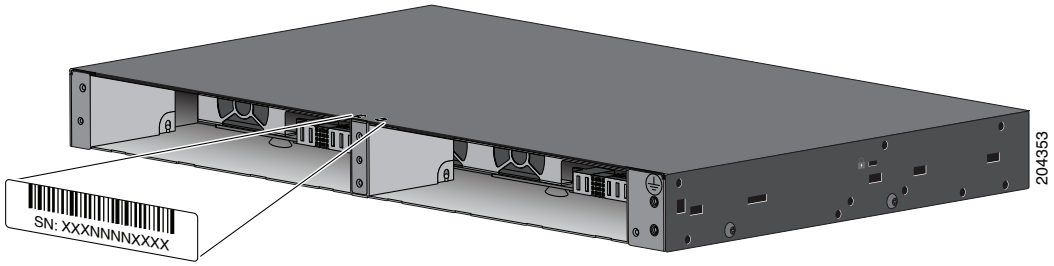

Figure 4-3 Serial Number Location on the Cisco ME 3400EG-2CS-A