CHAPTER 4

Troubleshooting

This chapter describes these Catalyst 3750-E and Catalyst 3560-E switch troubleshooting topics:

Diagnosing Problems

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

Check Switch POST Results

As the switch powers on, it begins the power-on self-test (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 switch status LEDs turn green. The System LED blinks green, and the other LEDs remain continuous green.

When POST completes successfully, the System LED remains green. The RPS LED remains green for some time and then returns to its operating status. The other LEDs turn off and return to their operating status. If the switch fails POST, the System and Ethernet management port LEDs are amber.

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

Check Switch LEDs

If you have physical access to the switch, look at the port LEDs for troubleshooting information about the switch. See the "LEDs" section on page 1-6 for a description of the LED colors and their meanings.

Check Switch Connections

Review this section when troubleshooting switch connection problems.

Bad or Damaged Cable

Always check 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). You should:

- Check or swap 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 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.
- Catalyst 3750-E switch StackWise cable: remove and inspect the cable and StackWise port for bent pins or damaged connectors. If the StackWise cable is bad, replace it with a known good 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 Mbps UTP connections. Use either Category 5, Category 5e, or Category 6 UTP for 10/100 or 10/100/1000 Mbps 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 more information about cabling, see the "10-Gigabit Ethernet X2 Transceiver Module Cable Specifications" section on page B-5 and the "SFP Module Cable Specifications" section on page B-6.
- 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 the 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 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 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.
- Check for loose connections. Sometimes a cable appears to be seated, but is not. Disconnect the cable and then reconnect it.

PoE Connections

When a powered device is connected to PoE port, but no power is received, you should:

- Use the Mode button to show the PoE status for all ports. See Table 1-9 and Table 1-10 for a description of the LEDs and their meanings.
- Check the port status by using the **show interfaces** privileged EXEC command to check the port error-disabled, disabled, or shutdown status. Re-enable the port if necessary.
- Verify that the power supply installed in the switch meets the power requirements of your connected devices. See the "Power-Supply Modules" section on page 1-15 for more information.
- Check the cable type. Many legacy powered devices, including older Cisco IP phones and access points that do not fully support IEEE 802.3af, might not support PoE when connected to the switch by a crossover cable. Replace the crossover cable with a straight-through cable.

Caution PoE faults are caused when noncompliant cabling or powered devices are connected to a PoE port. Only standard-compliant cabling can be used to connect Cisco pre-standard IP phones and wireless access points or IEEE 802.3af-compliant devices to PoE ports. (You must remove a cable or device that causes a PoE fault from the network.)

Transceiver Issues

Use only Cisco X2 transceiver modules and 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 X2 transceiver, Cisco TwinGig Converter module, or SFP module. Exchange suspect module with known good module. Verify that the module is supported on this platform. (The switch release notes on Cisco.com list the X2 and SFP modules that the switch supports.)
- Use the **show interfaces** privileged EXEC command to check the port or module error-disabled, disabled, or shutdown status. Re-enable the port if needed.
- Make sure that all fiber connections are properly cleaned and securely connected.
- For CX4 module connections, make sure that cable routing does not violate the minimum allowed cable bend radius. See the module documentation for specific cabling requirements.
- For LX4 modules, a mode conditioning patch is recommended for MMF applications.

Port and Interface Settings

An obvious but sometimes overlooked cause of port connectivity failure is a disabled port. Verify that the port or interface is not disabled or powered down for some reason. If a port or 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

port. Use the **show interfaces** privileged EXEC command to check the port or interface error-disabled, disabled, or shutdown status on both sides of the connection. If needed, re-enable the port or the interface.

Ping End Device

Check the end device by pinging 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 see 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 look like port or interface problems. In this situation, the switch bandwidth is used over and over again by the same frames, leaving little room for legitimate traffic.

Loops can be caused by a unidirectional link. A unidirectional link occurs whenever the traffic sent by the switch is received by its neighbor, but the traffic from the neighbor is not received by the switch. A broken fiber-optic cable, other cabling, or a port issue could cause this one-way communication.

You can enable UniDirectional Link Detection (UDLD) on the switch to help identify difficult-to-find unidirectional link problems. UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about enabling UDLD on the switch, see the “Understanding UDLD” section in the software configuration guide for this release.

Check Switch Performance

Review this section when troubleshooting switch performance problems.

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 indicate 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. This can happen when manually setting the speed and duplex, or from autonegotiation issues between the two devices. A mismatch occurs under these circumstances:

- 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 performance and ensure a link, follow one of these guidelines when changing 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 NIC Cards

Problems sometimes occur between the switch and third-party network interface cards (NICs). By default, the switch ports and interfaces are set to autonegotiate. It is common for devices like laptops or other devices to be set to autonegotiate as well, 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 card. You can resolve this by upgrading the NIC card driver to the latest version available from the manufacture.

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 "Cable and Adapter Specifications" section on page B-5 for cabling guidelines.

How to Clear the Switch IP Address and Configuration

If you have configured a new switch with a wrong IP address, or if all of the switch LEDs start blinking when you are trying to enter Express Setup mode, you can clear the IP address that is configured on the switch.

Note 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.

Follow these steps to return your switch to the factory default settings:

1. Press and hold the Mode button (Figure 1-1 on page 1-3).

   The switch LEDs begin blinking after about 2 seconds. If the switch is not configured, the LEDs above the mode button turn green. You can omit this step and run Express Setup to configure the switch.

2. Continue holding down the Mode button. The LEDs stop blinking after an additional 8 seconds, and then the switch reboots.

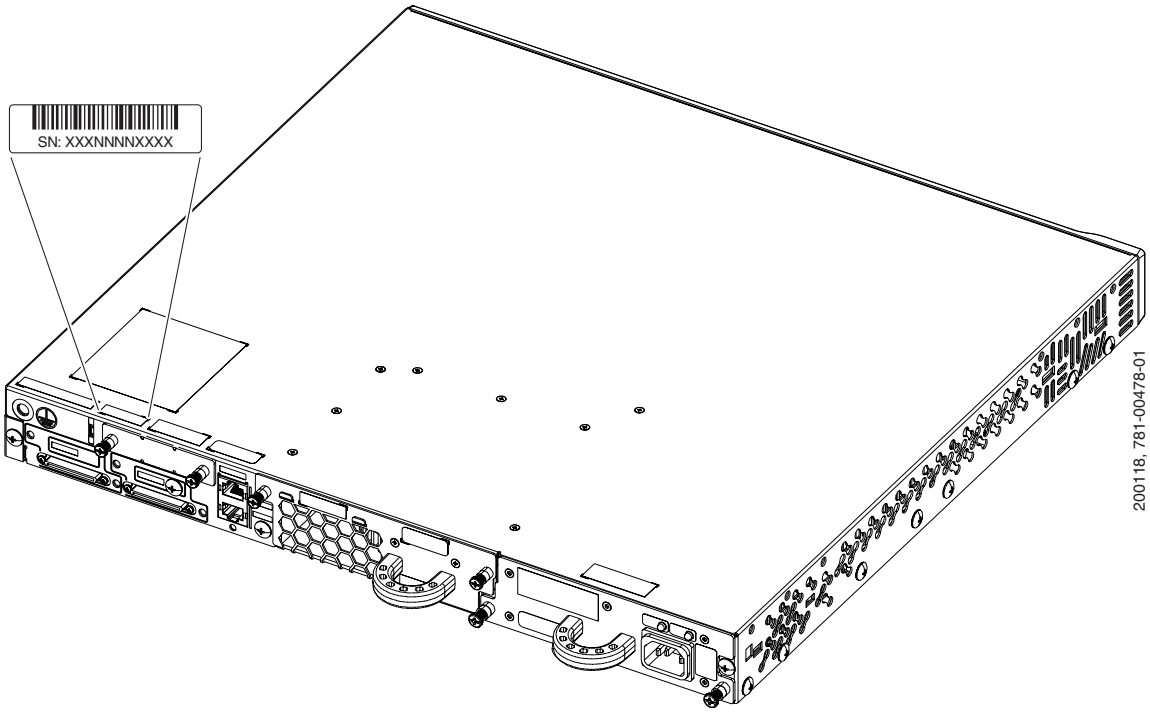
The switch now behaves like an unconfigured switch. You can configure the switch by using Express Setup as described in the switch getting started guide that is included with the switch.

You can also configure the switch by using the CLI setup procedure described in the Configuring the Switch with the CLI-Based Setup Program appendix.

Finding the Switch Serial Number

If you contact Cisco Technical Assistance, you need to know the serial number of your switch. See Figure 4-1 to find the serial number on your switch. You can also use the **show version** privileged EXEC command to get the switch serial number.

Figure 4-1 Switch Serial Number Location



How to Replace a Failed Stack Member

If you need to replace a failed stack member, you can hot swap or replace the switch by following this procedure (only Catalyst 3750-E switches):

1. Get a replacement switch that has the same model number as the failed switch.
2. Power down the failed switch.
3. Make sure the replacement switch is powered off, and then connect the replacement switch to the stack.

   If you had manually set the member numbers for any members in the stack, you need to manually assign the replacement switch with the same member number as the failed switch. To manually assign the member number, see the switch software configuration guide.
4. Make the same Gigabit Ethernet connections on the replacement switch that were on the failed switch.

5. Reinstall any modules and cable connections.
6. Power on the replacement switch.

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