

Troubleshooting

- Diagnosing Problems, on page 1
- Switch LEDs, on page 1
- Switch Connections, on page 1
- Switch Performance, on page 3
- Reset the Switch, on page 4
- Recovering Passwords, on page 5
- Finding the Switch Serial Number, on page 5

Diagnosing Problems

The switch LEDs provide troubleshooting information about the switch. They show port-connectivity problems and overall switch performance. You can also get statistics from the Web UI, the CLI, or an SNMP workstation. See the software configuration guides for Cisco Catalyst IE3100 Rugged Series Switches or the documentation that came with your SNMP application for details.

Switch LEDs

Look at the port LEDs information when troubleshooting the switch. See the LED information in the chapter Cisco Catalyst IE3100 Rugged Series Switches 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 problem because the port has many packet errors or it constantly flaps (loses and regains link).

- 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 media convertors (fiber-optic-to-copper).
- Try the cable in another port to see if the problem follows the cable.

Ethernet and Fiber-Optic Cables

Make sure that you have the correct cable:

- 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, 10/100/1000 Mb/s, and PoE connections.
- Verify that you have the correct fiber-optic cable for the distance and port type. Make sure that the connected device ports match and use the same type encoding, optical frequency, and fiber type.
- Determine if a copper crossover cable was used when a straight-through was required or the reverse. Enable auto-MDIX on the switch, or replace the cable.

Link Status

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

A port LED that is on does not guarantee that the cable is functional. It might have encountered physical stress, causing 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 the chapter Cables and Connectors in this guide for information.
- Look for loose connections. Sometimes a cable appears to be seated but is not. Disconnect the cable, and then reconnect it.

10/100/1000 Port Connections

If a port appears to malfunction, complete the following steps.

- Verify the status of all ports by checking the LEDs. For more information, see information about LEDs in the chapter Cisco Catalyst IE3100 Rugged Series Switches in this guide.
- Use the **show interfaces** privileged EXEC command to see if the port is error-disabled, disabled, or shut down. Re-enable the port if necessary.
- Verify the cable type.

SFP Module

Use only Cisco SFP modules. Each Cisco module has an internal serial EEPROM that is encoded with security information. This encoding verifies that the module meets the requirements for the switch.

- Inspect the SFP module. Exchange the suspect module with a 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. Reenable the port if needed.
- Make sure that all fiber-optic connections are clean and securely connected.

Interface Settings

Verify that the interface is not disabled or powered off. If an interface is manually shut down on either side of the link, it does not come up until you reenable the interface. Use the **show interfaces** privileged EXEC command to see if the interface is error-disabled, disabled, or shut down on either side of the connection. If needed, reenable the interface.

Ping 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.

A unidirectional link can cause loops. It occurs when the traffic sent by the switch is received by the neighbor, but the traffic from the neighbor is not received by the switch. A broken cable, other cabling problems, or a port issue can cause this one-way communication.

You can enable UniDirectional Link Detection (UDLD) on the switch to help identify unidirectional link problems. For information about enabling UDLD on the switch, see the “Understanding UDLD” section in the switch software configuration guide on Cisco.com.

Switch Performance

Speed, Duplex, and Autonegotiation

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

A common issue occurs when duplex and speed 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 the speed settings.

- Let both ports autonegotiate both speed and duplex.
- Manually set the speed and duplex parameters for the interfaces on both ends of the connection.
- If a remote device does not autonegotiate, use the same duplex settings on the two ports. The speed parameter adjusts itself even if the connected port does not autonegotiate.

Reset the Switch

These are reasons why you might want to reset the switch to the factory default settings:

- You installed the switch in your network and cannot connect to it because you assigned the wrong IP address.
- You want to reset the password on the switch.

Note Resetting the switch deletes the configuration and reboots the switch.

Caution If you press the Express Setup button when you power on, the automatic boot sequence stops, and the switch enters bootloader mode.

Attention :

Si vous appuyez sur le bouton de configuration express lors de la mise sous tension, la séquence de démarrage automatique s'arrête et le commutateur passe en mode de chargeur de démarrage.

To reset the switch, complete the following steps.

Procedure

Step 1 Press and hold the Express Setup button for 15 to 20 seconds with a paper clip or similar object.

The button is recessed behind a small hole in the faceplate. The Express Setup LED turns green after the switch reboots.

The switch reboots and returns to the manufacturing default configuration.

Step 2 Press the Express Setup button again for 3 seconds.

A switch 10/100/100 Ethernet port blinks green.

What to do next

The switch now behaves like an unconfigured switch. You can configure the switch by using the CLI setup procedure that is described in the Configuring the Switch with the CLI-Based Setup Program chapter in this guide. You can also configure the switch by using Express Setup as described in the Running Express Setup chapter in this guide.

Recovering Passwords

The default configuration for the switch allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process during power-on and by entering a new password. These recovery procedures require that you have physical access to the switch.

Note On these devices, a system administrator can disable some of the functionality of this feature by allowing an end user to reset a password only by agreeing to return to the default configuration. If you are an end user trying to reset a password when password recovery has been disabled, a status message reminds you to return to the default configuration during the recovery process.

See Reset the Switch, on page 4 in this guide for instructions on resetting the switch and entering a new password.

Finding the Switch Serial Number

If you contact Cisco Technical Assistance, you must know the serial number of your switch. You can also use the **show version** privileged EXEC command to obtain the switch serial number.

Also, the Serial Number for the switch is printed on the device label, on the device itself.