

Troubleshooting

- Diagnosing Issues, on page 1
- Reset the Switch, on page 4
- Emergency Recovery Installation, on page 5
- Secure Data Wipe, on page 5
- Locate the Switch Serial Number, on page 6
- How to Recover Passwords, on page 6

Diagnosing Issues

The switch LEDs provide troubleshooting information about the switch. They show boot failures, port-connectivity problems, and overall switch performance. You can also get statistics from Web UI, the CLI, or an SNMP workstation. See the Cisco IE3500, IE3505 Rugged Series Switch Software Configuration Guide, or the documentation that came with your SNMP application for details.

Switch LEDs

Look at the port LEDs when troubleshooting the switch. See LEDs 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 even though 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 Cable and Connectors for information.
- Look for loose connections. Sometimes a cable appears to be seated but is not. Disconnect the cable, and then reconnect it.

10/100/1G Port Connections

If a port appears to malfunction:

- Verify the status of all ports by checking the LEDs. For more information, see Switch LEDs, on page 1.
- Use the **show interfaces** EXEC command to see if the port is error-disabled, disabled, or shut down. Reenable 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.

Autonegotiation and Network Interface Cards

Problems sometimes occur between the switch and third-party network interface cards (NICs). By default, the switch ports and interfaces autonegotiate. Laptops or other devices are commonly set to autonegotiate, yet sometimes 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 the NIC. You can resolve this by upgrading the NIC driver to the latest 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 Cables and Adapters.

Reset the Switch

These are reasons why you might want to reset the switch startup configuration to factory defaults:

- 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. To securely erase all data, see Secure Data Wipe, on page 5.

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

To reset the switch:

Procedure

Step 1 Press and hold the Express Setup button (recessed behind a small hole in the faceplate) for about 15 seconds with a paper clip or similar object.

The Express Setup LED will blink red/green when its recessed button has been held down long enough.

Step 2 The switch reboots. The system LED turns green after the switch completes rebooting.

Step 3 Press the Express Setup button again for 3 seconds. A switch Ethernet port blinks green.

The switch now behaves like an unconfigured switch. You can configure the switch by using the CLI setup procedure described in Configure Switch using CLI.

Emergency Recovery Installation

Attention Emergency Recovery image is installed at manufacturing and is not updateable in the field. It may contain security vulnerabilities, and may not support features that were added in subsequent IOS images.

The Emergency Recovery image is a version of IOS that is always present on the system. It is installed in the **emgy0:** partition, and is write-protected to prevent accidental deletion.

Use the **dir emgy0:** command to see the Emergency Recovery image, and then "**boot emgy0:**<*image name*> to boot.

When using the Emergency Recovery image, it is recommended to isolate the switch by disconnecting external network interfaces, blocking remote access, and so on.

Secure Data Wipe

Secure data wipe is used to remove confidential information from the switch.

This feature is supported in all license levels:

- IE3500
- IE3505

When a secure data wipe is performed most user accessible flash memories are erased, including:

- User configuration and passwords
- Cisco IOS XE image
- Embedded MultiMediaCard (eMMC)
- rommon variables
- TPM Secure Storage

Note The secure data wipe process clears contents from SD card and USB devices. Alternatively, you may manually erase or reformat external storage devices.

After a secure data wipe the switch will return to a rommon prompt with the factory-default settings.

Note If an sdflash/usbflash with a valid image inserted, the device will boot with the image in the external media based on the boot precedence. The device will be in rommon only if no external media with an image is inserted in the device.

Perform Secure Data Wipe

To enable secure data wipe, enter the **factory-reset all secure** command in priviledged exec mode, as shown in the following example:

```
Switch#factory-reset ?
  all                 All factory reset operations
  keep-licensing-info  Keep license usage info
Switch#factory-reset all ?
secure  Securely reset all
Switch#factory-reset all secure
The factory reset operation is irreversible for securely reset all. Are you sure? [confirm]Y
```

factory-reset command options:

- **factory-reset all**—Remove everything from flash
- **factory-reset keep-licensing-info**—Keep the licensing information after factory reset and remove everything else from flash.
- **factory-reset all secure** —Remove everything from flash, and also unmount and sanitize the partitions before mounting back. This ensures that the data from those partitions cannot be recovered.



Important The **factory-reset all secure** operation may take hours. Please do not power cycle.

To check the log after the switch executes the command, boot up IOS XE and enter the following **show** command:

```
Switch#show platform software factory-reset secure log
Factory reset log:
#CISCO DATA SANITIZATION REPORT:# IE3200
Purge ACT2 chip at 12-08-2022, 15:17:28
ACT2 chip Purge done at 12-08-2022, 15:17:29
mtd and backup flash wipe start at 12-08-2022, 15:17:29
mtd and backup flash wipe done at 12-08-2022, 15:17:29.
```

Locate the Switch Serial Number

If you contact Cisco Technical Assistance, you must know the serial number of your switch. You can 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.

How to Recover 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 for the procedure to reset the switch and enter a new password.