Troubleshooting

Troubleshooting

This chapter provides troubleshooting recommendations.

Diagnosing Problems

The switch LEDs provide troubleshooting information about the switch. They show boot fast failures, port-connectivity problems, and overall switch performance. You can also get statistics from Device Manager, the CLI, or an SNMP workstation.

Switch Connections

Bad or Damaged Cable

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 cable with a known good cable.
- Look for broken or missing pins on cable connectors.
- Rule out any bad patch panel connections or media converters between the source and the destination. If possible, bypass the patch panel.
- Try the cable in another port to see if the problem follows 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.
- Look for loose connections. Sometimes a cable appears to be seated but is not. Disconnect the cable, and then reconnect it.

10/100 and 10/100/1000 Port Connections

If a port appears to malfunction:

- Verify the status of all ports. See Table 1-1 for descriptions of the LEDs and their meanings.
- Use the **show interfaces** privileged EXEC command to see if the port is error-disabled, disabled, or shut down. Reenable the port if necessary.
- Verify the cable type.

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 notification that the traffic was received 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 “Information About UDLD” section in the IOS-XE Software Configuration guide for the Cisco Catalyst IE 3x00 Switches, 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, a common issue when duplex and speed settings are mismatched between 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 to the same speed and duplex mode. If this does not solve the problem, there could be a problem with the firmware or software on the NIC. You might 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.

Resetting the Switch

Resetting the switch deletes the configuration and reboots the switch.

Reasons why you might want to reset the switch to the factory default settings include:

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

To reset the switch:

Procedure

Step 1 Press and hold the Express Setup button for 15 seconds or more. The switch reboots. The system led turns green and the expres setup led starts to blink green.

Step 2 Press the Express Setup button again for 1-3 seconds. LED for port 1/1 blinks green.

The switch now behaves like a factory-default configured switch. Go to section above on Express Setup to complete re-install.

Enabling Secure Data Wipe

Secure data wipe is a Cisco wide initiative to ensure storage devices on all IOS XE based platforms are properly purged using NIST SP 800-88r1 compliant secure erase commands.

This feature is supported in Cisco IOS XE 17.10.1 and later on the following IoT switches for all license levels:

- IE3200
- IE3300
- IE3400
- IE3400H
- ESS3300

When secure data wipe is enabled, everything in internal flash memory is erased, including:

- User configuration and passwords
- Cisco IOS XE image
- Embedded MultiMediaCard (eMMC)
- rommon variables
- ACT2 Secure Storage

Note Secure erase does not clear the SD card or USB device contents. You must manually erase or reformat external storage devices.

The switch will be in rommon prompt with default factory settings (baud rate 9600) after the command is executed. The internal flash memory will not get formatted until the IOS image is rebooted.

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.

Performing a 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.
```

How to Recover Passwords

Password recovery is a feature that a system administrator can enable or disable. If password recovery is disabled, the only way to recover from a lost or forgotten password is to clear the switch configuration entirely. For this procedure, see the "Resetting the Switch" section.

Troubleshooting Express Setup

This section provides troubleshooting tips for the initial switch configuration.

Checklist	Recommendation
Was the SETUP LED blinking when you pressed the Express Setup button?	If no, or you are not sure, restart the switch. Make sure that the SETUP LED is blinking when you press the Express Setup button.
Did you connect your PC to the wrong switch port?	Verify that you are connected to the switch port with the blinking LED.
Did you start a browser session on your PC before the SETUP LED was solid green?	If yes, or you are not sure, restart the switch, and repeat the Express Setup procedure.
Did you start a browser session on your PC and the setup page did not appear?	If the window does not appear, enter a URL in your browser, such as *Cisco.com* or another well known website.
Did you have a pop-up blocker running on your PC when you connected to the switch port?	If yes, disconnect the cable from the switch port, disable the pop-up blocker, press the Express Setup button, and reconnect the cable to the blinking Ethernet port.

Checklist	Recommendation
Did you have proxy settings enabled in your browser software when you connected to the switch port?	If yes, disconnect the cable from the switch port, disable the proxy settings, press the Express Setup button, and reconnect the cable to the blinking Ethernet port.
Did you have a wireless client running on your PC when you connected to the switch port?	If yes, disconnect the cable from the switch port, disable the wireless client, press the Express Setup button, and reconnect the cable to the blinking Ethernet port.
Do you need to change the switch IP address after you have already completed the initial setup?	Go to the **Configure > Express Setup** Device Manager screen to change the switch IP address. For more information about changing the switch IP address, see the Cisco IE 2000 Switch Software Configuration Guide at Cisco.com.

Finding the Switch Serial Number

If you contact Cisco Technical Assistance, you need to know the serial number of your switch. The serial number is on the compliance label on left hand side under the removeable door. You can also use the **show version** privileged EXEC command to obtain the switch serial number.