Troubleshooting the Software Configuration

This chapter describes how to identify and resolve software problems related to the Cisco IOS software on the switch. Depending on the nature of the problem, you can use the command-line interface (CLI), Device Manager, or Network Assistant to identify and solve problems.

Additional troubleshooting information, such as LED descriptions, is provided in the hardware installation guide.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Troubleshooting the Software Configuration

Recovering from a Software Failure

Switch software can be corrupted during an upgrade, by downloading the wrong file to the Switch, and by deleting the image file. In all of these cases, the Switch does not pass the power-on self-test (POST), and there is no connectivity.

This procedure uses the Xmodem Protocol to recover from a corrupt or wrong image file. There are many software packages that support the Xmodem Protocol, and this procedure is largely dependent on the emulation software that you are using.

This recovery procedure requires that you have physical access to the switch.

SUMMARY STEPS

1. From your PC, download the software image tar file (*image_filename.tar*) from *Cisco.com*.
2. Extract the bin file from the tar file.
3. Connect your PC with terminal-emulation software supporting the Xmodem Protocol to the switch console port.
4. Set the line speed on the emulation software to 9600 baud.
5. Unplug the Switch power cord.
6. Press the **Mode** button, and at the same time, reconnect the power cord to the Switch.
7. Initialize the flash file system:
8. If you had set the console port speed to anything other than 9600, it has been reset to that particular speed. Change the emulation software line speed to match that of the switch console port.
9. Load any helper files:
10. Start the file transfer by using the Xmodem Protocol.
11. After the Xmodem request appears, use the appropriate command on the terminal-emulation software to start the transfer and to copy the software image into flash memory.
12. Boot the newly downloaded Cisco IOS image.
13. Use the **archive download-sw** privileged EXEC command to download the software image to the Switch.
14. Use the **reload** privileged EXEC command to restart the Switch and to verify that the new software image is operating properly.
15. Delete the flash:*image_filename.bin* file from the Switch.

DETAILED STEPS

	Command or Action	Purpose
Step 1	From your PC, download the software image tar file (*image_filename.tar*) from *Cisco.com*.	The Cisco IOS image is stored as a bin file in a directory in the tar file. For information about locating the software image files on *Cisco.com*, see the release notes.

Step 2	Extract the bin file from the tar file.	If you are using Windows, use a zip program that can read a tar file. Use the zip program to navigate to and extract the bin file.
		If you are using UNIX, follow these steps:
		• Display the contents of the tar file by using the tar -tvf <image_filename.tar> UNIX command.
		`switch% tar -tvf image_filename.tar`
		• Locate the bin file, and extract it by using the tar -xvf <image_filename.tar> <image_filename.bin> UNIX command.
		`switch% tar -xvf image_filename.tar image_filename.bin`
		`x image_name.bin, 3970586 bytes, 7756 tape blocks`
		• Verify that the bin file was extracted by using the ls -l <image_filename.bin> UNIX command.

	Command or Action	Purpose
		`switch% ls -l image_filename.bin` `-rw-r--r-- 1 boba 3970586 Apr 21 12:00 image_name.bin`
Step 3	Connect your PC with terminal-emulation software supporting the Xmodem Protocol to the switch console port.	
Step 4	Set the line speed on the emulation software to 9600 baud.	
Step 5	Unplug the Switch power cord.	

Step 6	Press the **Mode** button, and at the same time, reconnect the power cord to the Switch.	You can release the **Mode** button a second or two after the LED above port 1 goes off. Several lines of information about the software appear with instructions:
		`The system has been interrupted prior to initializing the flash file system. The following commands will initialize the flash file system, and finish loading the operating system software#`
		
		`flash_init`
		`load_helper`
		`boot`

Step 7	Initialize the flash file system:	`switch: flash_init`
Step 8	If you had set the console port speed to anything other than 9600, it has been reset to that particular speed. Change the emulation software line speed to match that of the switch console port.	
Step 9	Load any helper files:	`switch: load_helper`
Step 10	Start the file transfer by using the Xmodem Protocol.	`switch: copy xmodem: flash:image_filename.bin`
Step 11	After the Xmodem request appears, use the appropriate command on the terminal-emulation software to start the transfer and to copy the software image into flash memory.	
Step 12	Boot the newly downloaded Cisco IOS image.	`switch: boot flash:image_filename.bin`
Step 13	Use the **archive download-sw** privileged EXEC command to download the software image to the Switch.	
Step 14	Use the **reload** privileged EXEC command to restart the Switch and to verify that the new software image is operating properly.	
Step 15	Delete the flash:*image_filename.bin* file from the Switch.	

Recovering from a Lost or Forgotten Password

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 Switch, 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 shows this during the recovery process.

You enable or disable password recovery by using the **service password-recovery** global configuration command.

Follow the steps in this procedure if you have forgotten or lost the switch password.

SUMMARY STEPS

1. Connect a terminal or PC with terminal-emulation software to the switch console port.
2. Set the line speed on the emulation software to 9600 baud.
3. Power off the switch.
4. Reconnect the power cord to the Switch or the stack's active switch. Within 15 seconds, press the **Mode** button while the System LED is still flashing green. Continue pressing the **Mode** button until the System LED turns briefly amber and then solid green; then release the **Mode** button.
   - If you see a message that begins with this, proceed to the *Procedure with Password Recovery Enabled* section, and follow the steps.

     ```
     The system has been interrupted prior to initializing the flash file system. The
     following commands will initialize the flash file system
     ```

   - If you see a message that begins with this, proceed to the *Procedure with Password Recovery Disabled* section, and follow the steps.

     ```
     The password-recovery mechanism has been triggered, but is currently disabled.
     ```

5. After recovering the password, reload the switch:

DETAILED STEPS

	Command or Action	Purpose
Step 1	Connect a terminal or PC with terminal-emulation software to the switch console port.	
Step 2	Set the line speed on the emulation software to 9600 baud.	
Step 3	Power off the switch.	

	Command or Action	Purpose

Step 4	Reconnect the power cord to the Switch or the stack's active switch. Within 15 seconds, press the **Mode** button while the System LED is still flashing green. Continue pressing the **Mode** button until the System LED turns briefly amber and then solid green; then release the **Mode** button.
	• If you see a message that begins with this, proceed to the *Procedure with Password Recovery Enabled* section, and follow the steps.
	`The system has been interrupted prior to initializing the flash file system. The following commands will initialize the flash file system`
	• If you see a message that begins with this, proceed to the *Procedure with Password Recovery Disabled* section, and follow the steps.
	`The password-recovery mechanism has been triggered, but is currently disabled.`
		Several lines of information about the software appear with instructions, informing you if the password recovery procedure has been disabled or not.

Step 5	After recovering the password, reload the switch:	`Switch> reload` `Proceed with reload? [confirm] y`

Procedure with Password Recovery Enabled

If the password-recovery mechanism is enabled, this message appears:

```
The system has been interrupted prior to initializing the flash file system. The following
commands will initialize the flash file system, and finish loading the operating system
software:

flash_init
load_helper
boot
```

SUMMARY STEPS

1. Initialize the flash file system:
2. If you had set the console port speed to anything other than 9600, it has been reset to that particular speed. Change the emulation software line speed to match that of the Switch console port.
3. Load any helper files:
4. Display the contents of flash memory:
5. Rename the configuration file to config.text.old.
6. Boot up the system:
7. At the Switch prompt, enter privileged EXEC mode:
8. Rename the configuration file to its original name:
9. Copy the configuration file into memory:
10. Enter global configuration mode:
11. Change the password:
12. Return to privileged EXEC mode:

13. Write the running configuration to the startup configuration file:
14. Reload the Switch or switch stack:

DETAILED STEPS

	Command or Action	Purpose
Step 1	Initialize the flash file system:	`switch: flash_init`
Step 2	If you had set the console port speed to anything other than 9600, it has been reset to that particular speed. Change the emulation software line speed to match that of the Switch console port.	
Step 3	Load any helper files:	`switch: load_helper`

Step 4	Display the contents of flash memory:	`switch: dir flash:`
		The Switch file system appears:
		`Directory of flash:`
		`13 drwx 192 Mar 01 1993 22:30:48 switch_image`
		`11 -rwx 5825 Mar 01 1993 22:31:59 config.text`
		`18 -rwx 720 Mar 01 1993 02:21:30 vlan.dat`
		`16128000 bytes total (10003456 bytes free)`

Step 5	Rename the configuration file to config.text.old.	This file contains the password definition. `switch: rename flash:config.text flash:config.text.old`

Step 6	Boot up the system:	`switch: boot`
		You are prompted to start the setup program. Enter N at the prompt:
		`Continue with the configuration dialog? [yes/no]: N`

Step 7	At the Switch prompt, enter privileged EXEC mode:	`Switch> enable`
Step 8	Rename the configuration file to its original name:	`Switch# rename flash:config.text.old flash:config.text` **Note** Before continuing to Step 9, power on any connected stack members and wait until they have completely initialized. Failure to follow this step can result in a lost configuration depending on how your Switch is set up.

Step 9	Copy the configuration file into memory:	`Switch# copy flash:config.text system:running-config`
		`Source filename [config.text]?`
		`Destination filename [running-config]?`
		Press Return in response to the confirmation prompts.
		The configuration file is now reloaded, and you can change the password.

Step 10	Enter global configuration mode:	`Switch# configure terminal`

	Command or Action	Purpose
Step 11	Change the password:	`Switch (config)# enable secret password` The secret password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, and allows spaces but ignores leading spaces.
Step 12	Return to privileged EXEC mode:	`Switch (config)# exit` `Switch#`
Step 13	Write the running configuration to the startup configuration file:	`Switch# copy running-config startup-config` The new password is now in the startup configuration. **Note** This procedure is likely to leave your Switch virtual interface in a shutdown state. You can see which interface is in this state by entering the show running-config privileged EXEC command. To re-enable the interface, enter the interface vlan vlan-id global configuration command, and specify the VLAN ID of the shutdown interface. With the Switch in interface configuration mode, enter the no shutdown command.
Step 14	Reload the Switch or switch stack:	`Switch# reload`

Procedure with Password Recovery Disabled

If the password-recovery mechanism is disabled, this message appears:

```
The password-recovery mechanism has been triggered, but
is currently disabled.  Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point.  However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default configuration (y/n)?
```

Caution Returning the Switch to the default configuration results in the loss of all existing configurations. We recommend that you contact your system administrator to verify if there are backup Switch and VLAN configuration files.

- If you enter **n** (no), the normal boot process continues as if the **Mode** button had not been pressed; you cannot access the boot loader prompt, and you cannot enter a new password. You see the message:

  ```
  Press Enter to continue........
  ```

- If you enter **y** (yes), the configuration file in flash memory and the VLAN database file are deleted. When the default configuration loads, you can reset the password.

Step 1 Choose to continue with password recovery and delete the existing configuration:

```
Would you like to reset the system back to the default configuration (y/n)? Y
```

Step 2 Display the contents of flash memory:

```
Switch: dir flash:
```

The Switch file system appears.

Step 3 Boot up the system:

```
Switch: boot
```

You are prompted to start the setup program. To continue with password recovery, enter **N** at the prompt:

```
Continue with the configuration dialog? [yes/no]: N
```

Step 4 At the Switch prompt, enter privileged EXEC mode:

```
Switch> enable
```

Step 5 Enter global configuration mode:

```
Switch# configure terminal
```

Step 6 Change the password:

```
Switch(config)# enable secret password
```

The secret password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, and allows spaces but ignores leading spaces.

Step 7 Return to privileged EXEC mode:

```
Switch(config)# exit
Switch#
```

Note Before continuing to Step 9, power on any connected stack members and wait until they have completely initialized.

Step 8 Write the running configuration to the startup configuration file:

```
Switch# copy running-config startup-config
```

The new password is now in the startup configuration.

Step 9 You must now reconfigure the Switch. If the system administrator has the backup Switch and VLAN configuration files available, you should use those.

Recovering from a Command Switch Failure

This section describes how to recover from a failed command Switch. You can configure a redundant command Switch group by using the Hot Standby Router Protocol (HSRP).

Note HSRP is the preferred method for supplying redundancy to a cluster.

If you have not configured a standby command Switch, and your command Switch loses power or fails in some other way, management contact with the member Switch is lost, and you must install a new command Switch. However, connectivity between Switch that are still connected is not affected, and the member Switch forward packets as usual. You can manage the members as standalone Switch through the console port, or, if they have IP addresses, through the other management interfaces.

You can prepare for a command Switch failure by assigning an IP address to a member Switch or another Switch that is command-capable, making a note of the command-switch password, and cabling your cluster to provide redundant connectivity between the member Switch and the replacement command Switch. These sections describe two solutions for replacing a failed command switch:

- Replacing a Failed Command Switch with a Cluster Member
- Replacing a Failed Command Switch with Another Switch

These recovery procedures require that you have physical access to the Switch.

For information on command-capable Switch, see the release notes.

Replacing a Failed Command Switch with a Cluster Member

To replace a failed command Switch with a command-capable member in the same cluster, follow these steps:

SUMMARY STEPS

1. Disconnect the command Switch from the member Switch, and physically remove it from the cluster.
2. Insert the member Switch in place of the failed command switch, and duplicate its connections to the cluster members.
3. Start a CLI session on the new command Switch.
4. At the Switch prompt, enter privileged EXEC mode:
5. Enter the password of the *failed command switch*.
6. Enter global configuration mode.
7. Remove the member Switch from the cluster.
8. Return to privileged EXEC mode.
9. Use the setup program to configure the Switch IP information. This program prompts you for IP address information and passwords. From privileged EXEC mode, enter **setup**, and press **Return**.
10. Enter Y at the first prompt.
11. Respond to the questions in the setup program.

12. When prompted for the **enable secret** and **enable** passwords, enter the passwords of the *failed command switch* again.
13. When prompted, make sure to enable the Switch as the cluster command Switch, and press **Return**.
14. When prompted, assign a name to the cluster, and press **Return**.
15. After the initial configuration displays, verify that the addresses are correct.
16. If the displayed information is correct, enter **Y**, and press **Return**.
17. Start your browser, and enter the IP address of the new command Switch.
18. From the Cluster menu, select **Add to Cluster** to display a list of candidate Switch to add to the cluster.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Disconnect the command Switch from the member Switch, and physically remove it from the cluster.	
Step 2	Insert the member Switch in place of the failed command switch, and duplicate its connections to the cluster members.	
Step 3	Start a CLI session on the new command Switch.	You can access the CLI by using the console port or, if an IP address has been assigned to the Switch, by using Telnet. For details about using the console port, see the Switch hardware installation guide.
Step 4	At the Switch prompt, enter privileged EXEC mode:	`Switch> enable` `Switch#`
Step 5	Enter the password of the *failed command switch*.	
Step 6	Enter global configuration mode.	`Switch# configure terminal` `Enter configuration commands, one per line. End with CNTL/Z.`
Step 7	Remove the member Switch from the cluster.	`Switch(config)# no cluster commander-address`
Step 8	Return to privileged EXEC mode.	`Switch(config)# end` `Switch#`

Step 9	Use the setup program to configure the Switch IP information. This program prompts you for IP address information and passwords. From privileged EXEC mode, enter **setup**, and press **Return**.	`Switch# setup`
		`--- System Configuration Dialog ---`
		`Continue with configuration dialog? [yes/no]: y`
		
		`At any point you may enter a question mark '?' for help.`
		`Use ctrl-c to abort configuration dialog at any prompt.`
		`Default settings are in square brackets '[]'.`
		
		`Basic management setup configures only enough connectivity`
		`for management of the system, extended setup will ask you`
		`to configure each interface on the system`
		
		`Would you like to enter basic management setup? [yes/no]:`

	Command or Action	Purpose

Step 10	Enter Y at the first prompt.	The prompts in the setup program vary depending on the member Switch that you selected to be the command switch:
		`Continue with configuration dialog? [yes/no]: y`
		or
		`Configuring global parameters:`
		If this prompt does not appear, enter **enable**, and press **Return**. Enter **setup**, and press **Return** to start the setup program.

Step 11	Respond to the questions in the setup program.	When prompted for the hostname, recall that on a command Switch, the hostname is limited to 28 characters; on a member Switch to 31 characters. Do not use *-n*, where *n* is a number, as the last characters in a hostname for any Switch. When prompted for the Telnet (virtual terminal) password, recall that it can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.
Step 12	When prompted for the **enable secret** and **enable** passwords, enter the passwords of the *failed command switch* again.	
Step 13	When prompted, make sure to enable the Switch as the cluster command Switch, and press **Return**.	
Step 14	When prompted, assign a name to the cluster, and press **Return**.	The cluster name can be 1 to 31 alphanumeric characters, dashes, or underscores.
Step 15	After the initial configuration displays, verify that the addresses are correct.	
Step 16	If the displayed information is correct, enter **Y**, and press **Return**.	If this information is not correct, enter **N**, press **Return**, and begin again at Step 9.
Step 17	Start your browser, and enter the IP address of the new command Switch.	
Step 18	From the Cluster menu, select **Add to Cluster** to display a list of candidate Switch to add to the cluster.	

Replacing a Failed Command Switch with Another Switch

To replace a failed command Switch with a Switch that is command-capable but not part of the cluster, follow these steps:

SUMMARY STEPS

1. Insert the new Switch in place of the failed command Switch, and duplicate its connections to the cluster members.
2. Start a CLI session on the new command Switch.
3. At the Switch prompt, enter privileged EXEC mode:

4. Enter the password of the *failed command switch*.
5. Use the setup program to configure the Switch IP information.
6. Enter **Y** at the first prompt.
7. Respond to the questions in the setup program.
8. When prompted for the **enable secret** and **enable** passwords, enter the passwords of the *failed command switch* again.
9. When prompted, make sure to enable the Switch as the cluster command Switch, and press **Return**.
10. When prompted, assign a name to the cluster, and press **Return**.
11. When the initial configuration displays, verify that the addresses are correct.
12. If the displayed information is correct, enter **Y**, and press **Return**.
13. Start your browser, and enter the IP address of the new command Switch.
14. From the Cluster menu, select **Add to Cluster** to display a list of candidate Switch to add to the cluster.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Insert the new Switch in place of the failed command Switch, and duplicate its connections to the cluster members.	
Step 2	Start a CLI session on the new command Switch.	You can access the CLI by using the console port or, if an IP address has been assigned to the Switch, by using Telnet. For details about using the console port, see the Switch hardware installation guide. For details about using the Ethernet management port, see the *Using the Ethernet Management Port section* and the hardware configuration guide.
Step 3	At the Switch prompt, enter privileged EXEC mode:	`Switch> enable` `Switch#`
Step 4	Enter the password of the *failed command switch*.	

Step 5	Use the setup program to configure the Switch IP information.	This program prompts you for IP address information and passwords. From privileged EXEC mode, enter **setup**, and press **Return**.
		`Switch# setup`
		`--- System Configuration Dialog ---`
		`Continue with configuration dialog? [yes/no]: y`
		
		`At any point you may enter a question mark '?' for help.`
		`Use ctrl-c to abort configuration dialog at any prompt.`
		`Default settings are in square brackets '[]'.`
		
		`Basic management setup configures only enough connectivity`
		`for management of the system, extended setup will ask you`
		`to configure each interface on the system`
		
		`Would you like to enter basic management setup? [yes/no]:`

	Command or Action	Purpose

Step 6	Enter **Y** at the first prompt.	The prompts in the setup program vary depending on the switch you selected to be the command Switch:
		`Continue with configuration dialog? [yes/no]: y`
		or
		`Configuring global parameters:`
		If this prompt does not appear, enter **enable**, and press **Return**. Enter **setup**, and press **Return** to start the setup program.

Step 7	Respond to the questions in the setup program.	When prompted for the hostname, recall that on a command Switch, the hostname is limited to 28 characters. Do not use *-n*, where *n* is a number, as the last character in a hostname for any Switch. When prompted for the Telnet (virtual terminal) password, recall that it can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.
Step 8	When prompted for the **enable secret** and **enable** passwords, enter the passwords of the *failed command switch* again.	
Step 9	When prompted, make sure to enable the Switch as the cluster command Switch, and press **Return**.	
Step 10	When prompted, assign a name to the cluster, and press **Return**.	The cluster name can be 1 to 31 alphanumeric characters, dashes, or underscores.
Step 11	When the initial configuration displays, verify that the addresses are correct.	
Step 12	If the displayed information is correct, enter **Y**, and press **Return**.	If this information is not correct, enter **N**, press **Return**, and begin again at Step 9.
Step 13	Start your browser, and enter the IP address of the new command Switch.	
Step 14	From the Cluster menu, select **Add to Cluster** to display a list of candidate Switch to add to the cluster.	

Recovering from Lost Cluster Member Connectivity

Some configurations can prevent the command Switch from maintaining contact with member Switch. If you are unable to maintain management contact with a member, and the member Switch is forwarding packets normally, check for these conflicts:

- A member Switch (Catalyst 3750, Catalyst 3560, Catalyst 3550, Catalyst 3500 XL, Catalyst 2970, Catalyst 2960, Catalyst 2950, Catalyst 2900 XL, Catalyst 2820, and Catalyst 1900 switch) cannot connect to the command Switch through a port that is defined as a network port.
- Catalyst 3500 XL, Catalyst 2900 XL, Catalyst 2820, and Catalyst 1900 member Switch must connect to the command Switch through a port that belongs to the same management VLAN.
- A member Switch (Catalyst 3750, Catalyst 3560, Catalyst 3550, Catalyst 2970, Catalyst 2960, Catalyst 2950, Catalyst 3500 XL, Catalyst 2900 XL, Catalyst 2820, and Catalyst 1900 Switch) connected to the

command Switch through a secured port can lose connectivity if the port is disabled because of a security violation.

Preventing Autonegotiation Mismatches

The IEEE 802.3ab autonegotiation protocol manages the Switch settings for speed (10 Mb/s, 100 Mb/s, and 1000 Mb/s, excluding SFP module ports) and duplex (half or full). There are situations when this protocol can incorrectly align these settings, reducing performance. 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.

Note 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.

Troubleshooting Power over Ethernet Switch Ports

- Disabled Port Caused by Power Loss
- Disabled Port Caused by False Link Up

Disabled Port Caused by Power Loss

If a powered device (such as a Cisco IP Phone 7910) that is connected to a PoE Switch port and powered by an AC power source loses power from the AC power source, the device might enter an error-disabled state. To recover from an error-disabled state, enter the **shutdown** interface configuration command, and then enter the **no shutdown** interface command. You can also configure automatic recovery on the Switch to recover from the error-disabled state.

On a Switch, the **errdisable recovery cause loopback** and the **errdisable recovery interval** *seconds* global configuration commands automatically take the interface out of the error-disabled state after the specified period of time.

Use these commands, described in the command reference for this release, to monitor the PoE port status:

- **show controllers power inline** privileged EXEC command
- **show power inline** privileged EXEC command
- **debug ilpower** privileged EXEC command

Disabled Port Caused by False Link-Up

If a Cisco powered device is connected to a port and you configure the port by using the **power inline never** interface configuration command, a false link-up can occur, placing the port into an error-disabled state. To take the port out of the error-disabled state, enter the **shutdown** and the **no shutdown** interface configuration commands.

You should not connect a Cisco powered device to a port that has been configured with the **power inline never** command.

Troubleshooting SFP Module Security and Identification

Cisco small form-factor pluggable (SFP) modules have a serial EEPROM that contains the module serial number, the vendor name and ID, a unique security code, and cyclic redundancy check (CRC). When an SFP module is inserted in the Switch, the Switch software reads the EEPROM to verify the serial number, vendor name and vendor ID, and recompute the security code and CRC. If the serial number, the vendor name or vendor ID, the security code, or CRC is invalid, the software generates a security error message and places the interface in an error-disabled state.

Note The security error message references the GBIC_SECURITY facility. The Switch supports SFP modules and does not support GBIC modules. Although the error message text refers to GBIC interfaces and modules, the security messages actually refer to the SFP modules and module interfaces.

If you are using a non-Cisco SFP module, remove the SFP module from the Switch, and replace it with a Cisco module. After inserting a Cisco SFP module, use the **errdisable recovery cause gbic-invalid** global configuration command to verify the port status, and enter a time interval for recovering from the error-disabled state. After the elapsed interval, the Switch brings the interface out of the error-disabled state and retries the operation. For more information about the **errdisable recovery** command, see the command reference for this release.

If the module is identified as a Cisco SFP module, but the system is unable to read vendor-data information to verify its accuracy, an SFP module error message is generated. In this case, you should remove and reinsert the SFP module. If it continues to fail, the SFP module might be defective.

Monitoring SFP Module Status

You can check the physical or operational status of an SFP module by using the **show interfaces transceiver** privileged EXEC command. This command shows the operational status, such as the temperature and the current for an SFP module on a specific interface and the alarm status. You can also use the command to check the speed and the duplex settings on an SFP module. For more information, see the **show interfaces transceiver** command in the command reference for this release.

Using Ping

- Understanding Ping
- Executing Ping

Ping

The Switch supports IP ping, which you can use to test connectivity to remote hosts. Ping sends an echo request packet to an address and waits for a reply. Ping returns one of these responses:

- Normal response—The normal response (*hostname* is alive) occurs in 1 to 10 seconds, depending on network traffic.
- Destination does not respond—If the host does not respond, a *no-answer* message is returned.
- Unknown host—If the host does not exist, an *unknown host* message is returned.
- Destination unreachable—If the default gateway cannot reach the specified network, a *destination-unreachable* message is returned.
- Network or host unreachable—If there is no entry in the route table for the host or network, a *network or host unreachable* message is returned.

Executing Ping

If you attempt to ping a host in a different IP subnetwork, you must define a static route to the network or have IP routing configured to route between those subnets.

IP routing is disabled by default on all Switch.

Note Though other protocol keywords are available with the **ping** command, they are not supported in this release.

Use this command to ping another device on the network from the Switch:

Command	Purpose
ping ip *host* | *address* `Switch# ping 172.20.52.3`	Pings a remote host through IP or by supplying the hostname or network address.

The below Table describes the possible ping character output.

Table 1: Ping Output Display Characters

Character	Description
!	Each exclamation point means receipt of a reply.
.	Each period means the network server timed out while waiting for a reply.
U	A destination unreachable error PDU was received.
C	A congestion experienced packet was received.
I	User interrupted test.
?	Unknown packet type.

Character	Description
&	Packet lifetime exceeded.

To end a ping session, enter the escape sequence (**Ctrl-^ X** by default). Simultaneously press and release the **Ctrl, Shift,** and **6** keys and then press the **X** key.

Using Layer 2 Traceroute

- Understanding Layer 2 Traceroute
- Usage Guidelines
- Displaying the Physical Path

Layer 2 Traceroute

The Layer 2 traceroute feature allows the switch to identify the physical path that a packet takes from a source device to a destination device. Layer 2 traceroute supports only unicast source and destination MAC addresses. Traceroute finds the path by using the MAC address tables of the Switch in the path. When the Switch detects a device in the path that does not support Layer 2 traceroute, the Switch continues to send Layer 2 trace queries and lets them time out.

The Switch can only identify the path from the source device to the destination device. It cannot identify the path that a packet takes from source host to the source device or from the destination device to the destination host.

Layer 2 Traceroute Guidelines

- Cisco Discovery Protocol (CDP) must be enabled on all the devices in the network. For Layer 2 traceroute to function properly, do not disable CDP.

  If any devices in the physical path are transparent to CDP, the switch cannot identify the path through these devices.

- A Switch is reachable from another Switch when you can test connectivity by using the **ping** privileged EXEC command. All Switch in the physical path must be reachable from each other.
- The maximum number of hops identified in the path is ten.
- You can enter the **traceroute mac** or the **traceroute mac ip** privileged EXEC command on a Switch that is not in the physical path from the source device to the destination device. All Switch in the path must be reachable from this switch.
- The **traceroute mac** command output shows the Layer 2 path only when the specified source and destination MAC addresses belong to the same VLAN. If you specify source and destination MAC addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.
- If you specify a multicast source or destination MAC address, the path is not identified, and an error message appears.
- If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.

- The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses belong to the same subnet. When you specify the IP addresses, the Switch uses the Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.
  - If an ARP entry exists for the specified IP address, the Switch uses the associated MAC address and identifies the physical path.
  - If an ARP entry does not exist, the Switch sends an ARP query and tries to resolve the IP address. If the IP address is not resolved, the path is not identified, and an error message appears.
- When multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port), the Layer 2 traceroute feature is not supported. When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.
- This feature is not supported in Token Ring VLANs.

Displaying the Physical Path

You can display physical path that a packet takes from a source device to a destination device by using one of these privileged EXEC commands:

- **tracetroute mac** [**interface** *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]
- **tracetroute mac ip** {*source-ip-address* | *source-hostname*} {*destination-ip-address* | *destination-hostname*} [**detail**]

For more information, see the command reference for this release.

IP Traceroute

You can use IP traceroute to identify the path that packets take through the network on a hop-by-hop basis. The command output displays all network layer (Layer 3) devices, such as routers, that the traffic passes through on the way to the destination.

Your Switch can participate as the source or destination of the **traceroute** privileged EXEC command and might or might not appear as a hop in the **traceroute** command output. If the Switch is the destination of the traceroute, it is displayed as the final destination in the traceroute output. Intermediate Switch do not show up in the traceroute output if they are only bridging the packet from one port to another within the same VLAN. However, if the intermediate Switch is a multilayer Switch that is routing a particular packet, this Switch shows up as a hop in the traceroute output.

The **traceroute** privileged EXEC command uses the Time To Live (TTL) field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a User Datagram Protocol (UDP) datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends an Internet Control Message Protocol (ICMP) time-to-live-exceeded message to the sender. Traceroute finds the address of the first hop by examining the source address field of the ICMP time-to-live-exceeded message.

To identify the next hop, traceroute sends a UDP packet with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the time-to-live-exceeded message to the source. This process continues until the

TTL is incremented to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

To learn when a datagram reaches its destination, traceroute sets the UDP destination port number in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram destined to itself containing a destination port number that is unused locally, it sends an ICMP *port-unreachable* error to the source. Because all errors except port-unreachable errors come from intermediate hops, the receipt of a port-unreachable error means that this message was sent by the destination port.

Executing IP Traceroute

Note Though other protocol keywords are available with the **traceroute** privileged EXEC command, they are not supported in this release.

Command	Purpose
traceroute ip *host* `Switch# traceroute ip 192.51.100.1`	Traces the path that packets take through the network.

Time Domain Reflector Guidelines

You can use the Time Domain Reflector (TDR) feature to diagnose and resolve cabling problems. When running TDR, a local device sends a signal through a cable and compares the reflected signal to the initial signal.

TDR can detect these cabling problems:

- Open, broken, or cut twisted-pair wires—The wires are not connected to the wires from the remote device.
- Shorted twisted-pair wires—The wires are touching each other or the wires from the remote device. For example, a shorted twisted pair can occur if one wire of the twisted pair is soldered to the other wire.

If one of the twisted-pair wires is open, TDR can find the length at which the wire is open.

Use TDR to diagnose and resolve cabling problems in these situations:

- Replacing a Switch
- Setting up a wiring closet
- Troubleshooting a connection between two devices when a link cannot be established or when it is not operating properly

Running TDR and Displaying the Results

To run TDR, enter the **test cable-diagnostics tdr interface** *interface-id* privileged EXEC command.

To display the results, enter the **show cable-diagnostics tdr interface** *interface-id* privileged EXEC command.

Debug Commands

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

All **debug** commands are entered in privileged EXEC mode, and most **debug** commands take no arguments.

Enabling Debugging on a Specific Feature

All **debug** commands are entered in privileged EXEC mode, and most **debug** commands take no arguments. For example, beginning in privileged EXEC mode, enter this command to enable the debugging for Switched Port Analyzer (SPAN):

```
Switch# debug span-session
```

The switch continues to generate output until you enter the **no** form of the command.

If you enable a **debug** command and no output appears, consider these possibilities:

- The switch might not be properly configured to generate the type of traffic you want to monitor. Use the **show running-config** command to check its configuration.
- Even if the switch is properly configured, it might not generate the type of traffic you want to monitor during the particular period that debugging is enabled. Depending on the feature you are debugging, you can use commands such as the TCP/IP **ping** command to generate network traffic.

To disable debugging of SPAN, enter this command in privileged EXEC mode:

```
Switch# no debug span-session
```

Alternately, in privileged EXEC mode, you can enter the undebug form of the command:

```
Switch# undebug span-session
```

To display the state of each debugging option, enter this command in privileged EXEC mode:

```
Switch# show debugging
```

Enabling All-System Diagnostics

Beginning in privileged EXEC mode, enter this command to enable all-system diagnostics:

```
Switch# debug all
```

Note Caution: Because debugging output takes priority over other network traffic, and because the **debug all** privileged EXEC command generates more output than any other **debug** command, it can severely diminish Switch performance or even render it unusable. In virtually all cases, it is best to use more specific **debug** commands.

The **no debug all** privileged EXEC command disables all diagnostic output. Using the **no debug all** command is a convenient way to ensure that you have not accidentally left any **debug** commands enabled.

Redirecting Debug and Error Message Output

By default, the network server sends the output from **debug** commands and system error messages to the console. If you use this default, you can use a virtual terminal connection to monitor debug output instead of connecting to the console port or the Ethernet management port.

Possible destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. The syslog format is compatible with 4.3 Berkeley Standard Distribution (BSD) UNIX and its derivatives.

Note Be aware that the debugging destination you use affects system overhead. When you log messages to the console, very high overhead occurs. When you log messages to a virtual terminal, less overhead occurs. Logging messages to a syslog server produces even less, and logging to an internal buffer produces the least overhead of any method.

For more information about system message logging, see *Configuring System Message Logging*.

Using the show platform forward Command

The output from the **show platform forward** privileged EXEC command provides some useful information about the forwarding results if a packet entering an interface is sent through the system. Depending upon the parameters entered about the packet, the output provides lookup table results and port maps used to calculate forwarding destinations, bitmaps, and egress information.

Note For more syntax and usage information for the **show platform forward** command, see the Switch command reference for this release.

Most of the information in the output from the command is useful mainly for technical support personnel, who have access to detailed information about the Switch application-specific integrated circuits (ASICs). However, packet forwarding information can also be helpful in troubleshooting.

Using the crashinfo Files

The crashinfo files save information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The switch writes the crash information to the console at the time of the failure. The switch creates two types of crashinfo files:

- Basic crashinfo file—The switch automatically creates this file the next time you boot up the Cisco IOS image after the failure.
- Extended crashinfo file—The switch automatically creates this file when the system is failing.

Basic crashinfo Files

The information in the basic file includes the Cisco IOS image name and version that failed, a list of the processor registers, and a stack trace. You can provide this information to the Cisco technical support representative by using the **show tech-support** privileged EXEC command.

Basic crashinfo files are kept in this directory on the flash file system:

flash:/crashinfo/.

The filenames are crashinfo_*n* where *n* is a sequence number.

Each new crashinfo file that is created uses a sequence number that is larger than any previously existing sequence number, so the file with the largest sequence number describes the most recent failure. Version numbers are used instead of a timestamp because the switches do not include a real-time clock. You cannot change the name of the file that the system will use when it creates the file. However, after the file is created, you can use the **rename** privileged EXEC command to rename it, but the contents of the renamed file will not be displayed by the **show stacks** or the **show tech-support** privileged EXEC command. You can delete crashinfo files by using the **delete** privileged EXEC command.

You can display the most recent basic crashinfo file (that is, the file with the highest sequence number at the end of its filename) by entering the **show stacks** or the **show tech-support** privileged EXEC command. You also can access the file by using any command that can copy or display files, such as the **more** or the **copy** privileged EXEC command.

Extended crashinfo Files

The Switch creates the extended crashinfo file when the system is failing. The information in the extended file includes additional information that can help determine the cause of the Switch failure. You provide this information to the Cisco technical support representative by manually accessing the file and using the **more** or the **copy** privileged EXEC command.

Extended crashinfo files are kept in this directory on the flash file system:

flash:/crashinfo_ext/.

The filenames are crashinfo_ext_*n* where *n* is a sequence number.

You can configure the Switch to not create the extended creashinfo file by using the **no exception crashinfo** global configuration command.

Using Memory Consistency Check Routines

The Switch runs memory consistency check routines to detect and correct invalid ternary content addressable memory (TCAM) table entries that can affect the performance of the Switch.

If the Switch cannot fix the error, it logs a system error message specifying the TCAM space where the error is located:

- Unassigned space: Unassigned TCAM table entries for the current SDM template.
- Hulc Forwarding TCAM Manager (HFTM) space: Related to the Layer 2 and Layer 3 forwarding tables.
- Hulc quality of service (QoS)/access control list (ACL) TCAM Manager (HQATM) space: Related to ACL and ACL-like tables such as QoS classification and policy routing.

The output from the **show platform tcam errors** privileged EXEC command provides information about the TCAM memory consistency integrity on the Switch.

Beginning in privileged EXEC mode, use the **show platform tcam errors** command to display the TCAM memory consistency check errors detected on the Switch:

Command	Purpose
show platform tcam errors	Displays TCAM memory consistency check errors in the HQATM, and HFTM.

Table 2: Definitions of Fields in TCAM Checker Output

Character	Description
Values	The number of invalid values.
Masks	The number of invalid masks.
Fixups	The number of initial attempts to fix the invalid values or masks.
Retries	The number of repeated attempts to fix the invalid values or masks.
Failures	The number of failed attempts to fix the invalid values or masks.

For more information about the **show platform tcam errors** privileged EXEC command, see the command reference for this release.

Troubleshooting CPU Utilization

This section lists some possible symptoms that could be caused by the CPU being too busy and shows how to verify a CPU utilization problem.

Possible Symptoms of High CPU Utilization

Excessive CPU utilization might result in these symptoms, but the symptoms might also result from other causes:

- Spanning tree topology changes
- EtherChannel links brought down due to loss of communication
- Failure to respond to management requests (ICMP ping, SNMP timeouts, slow Telnet or SSH sessions)
- UDLD flapping
- IP SLAs failures because of SLAs responses beyond an acceptable threshold
- DHCP or IEEE 802.1x failures if the switch does not forward or respond to requests

Layer 3 switches:

- Dropped packets or increased latency for packets routed in software
- BGP or OSPF routing topology changes
- HSRP flapping

Example: Verifying the Problem and Cause for High CPU Utilization

To determine if high CPU utilization is a problem, enter the **show processes cpu sorted** privileged EXEC command. Note the underlined information in the first line of the output example.

```
Switch# show processes cpu sorted
CPU utilization for five seconds: 8%/0%; one minute: 7%; five minutes: 8%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
309 42289103 752750 56180 1.75% 1.20% 1.22% 0 RIP Timers
140 8820183 4942081 1784 0.63% 0.37% 0.30% 0 HRPC qos request
100 3427318 16150534 212 0.47% 0.14% 0.11% 0 HRPC pm-counters
192 3093252 14081112 219 0.31% 0.14% 0.11% 0 Spanning Tree
143 8 37 216 0.15% 0.01% 0.00% 0 Exec
...
<output truncated>
```

This example shows normal CPU utilization. The output shows that utilization for the last 5 seconds is 8%/0%, which has this meaning:

- The total CPU utilization is 8 percent, including both time running Cisco IOS processes and time spent handling interrupts.
- The time spent handling interrupts is zero percent.

Table 3: Troubleshooting CPU Utilization Problems

Type of Problem	Cause	Corrective Action
Interrupt percentage value is almost as high as total CPU utilization value.	The CPU is receiving too many packets from the network.	Determine the source of the network packet. Stop the flow, or change the switch configuration. See the section on “Analyzing Network Traffic.”
Total CPU utilization is greater than 50% with minimal time spent on interrupts.	One or more Cisco IOS process is consuming too much CPU time. This is usually triggered by an event that activated the process.	Identify the unusual event, and troubleshoot the root cause. See the section on “Debugging Active Processes.”

Scenarios to Troubleshoot Power over Ethernet (PoE)

Table 4: Power over Ethernet Troubleshooting Scenarios

Symptom or Problem	Possible Cause and Solution
Only one port does not have PoE. Trouble is on only one switch port. PoE and non-PoE devices do not work on this port, but do on other ports.	Verify that the powered device works on another PoE port. Use the **show run**, or **show interface status** user EXEC commands to verify that the port is not shut down or error-disabled. **Note** Most switches turn off port power when the port is shut down, even though the IEEE specifications make this optional. Verify that the Ethernet cable from the powered device to the switch port is good: Connect a known good non-PoE Ethernet device to the Ethernet cable, and make sure that the powered device establishes a link and exchanges traffic with another host. Verify that the total cable length from the switch front panel to the powered device is not more than 100 meters. Disconnect the Ethernet cable from the switch port. Use a short Ethernet cable to connect a known good Ethernet device directly to this port on the switch front panel (not on a patch panel). Verify that it can establish an Ethernet link and exchange traffic with another host, or ping the port VLAN SVI. Next, connect a powered device to this port, and verify that it powers on. If a powered device does not power on when connected with a patch cord to the switch port, compare the total number of connected powered devices to the switch power budget (available PoE). Use the **show power inline** command to verify the amount of available power.

Symptom or Problem	Possible Cause and Solution
No PoE on all ports or a group of ports. Trouble is on all switch ports. Nonpowered Ethernet devices cannot establish an Ethernet link on any port, and PoE devices do not power on.	If there is a continuous, intermittent, or reoccurring alarm related to power, replace the power supply if possible it is a field-replaceable unit. Otherwise, replace the switch. If the problem is on a consecutive group of ports but not all ports, the power supply is probably not defective, and the problem could be related to PoE regulators in the switch. Use the **show log** privileged EXEC command to review alarms or system messages that previously reported PoE conditions or status changes. If there are no alarms, use the **show interface status** command to verify that the ports are not shut down or error-disabled. If ports are error-disabled, use the **shut** and **no shut** interface configuration commands to reenable the ports. Use the **show env power** and **show power inline** privileged EXEC commands to review the PoE status and power budget (available PoE). Review the running configuration to verify that **power inline never** is not configured on the ports. Connect a nonpowered Ethernet device directly to a switch port. Use only a short patch cord. Do not use the existing distribution cables. Enter the **shut** and **no shut** interface configuration commands, and verify that an Ethernet link is established. If this connection is good, use a short patch cord to connect a powered device to this port and verify that it powers on. If the device powers on, verify that all intermediate patch panels are correctly connected. Disconnect all but one of the Ethernet cables from switch ports. Using a short patch cord, connect a powered device to only one PoE port. Verify the powered device does not require more power than can be delivered by the switch port. Use the **show power inline** privileged EXEC command to verify that the powered device can receive power when the port is not shut down. Alternatively, watch the powered device to verify that it powers on. If a powered device can power on when only one powered device is connected to the switch, enter the **shut** and **no shut** interface configuration commands on the remaining ports, and then reconnect the Ethernet cables one at a time to the switch PoE ports. Use the **show interface status** and **show power inline** privileged EXEC commands to monitor inline power statistics and port status. If there is still no PoE at any port, a fuse might be open in the PoE section of the power supply. This normally produces an alarm. Check the log again for alarms reported earlier by system messages.

Symptom or Problem	Possible Cause and Solution
Cisco IP Phone disconnects or resets. After working normally, a Cisco phone or wireless access point intermittently reloads or disconnects from PoE.	Verify all electrical connections from the switch to the powered device. Any unreliable connection results in power interruptions and irregular powered device functioning such as erratic powered device disconnects and reloads. Verify that the cable length is not more than 100 meters from the switch port to the powered device. Notice what changes in the electrical environment at the switch location or what happens at the powered device when the disconnect occurs. Notice whether any error messages appear at the same time a disconnect occurs. Use the **show log** privileged EXEC command to review error messages. Verify that an IP phone is not losing access to the Call Manager immediately before the reload occurs. (It might be a network problem and not a PoE problem.) Replace the powered device with a non-PoE device, and verify that the device works correctly. If a non-PoE device has link problems or a high error rate, the problem might be an unreliable cable connection between the switch port and the powered device.
Non-Cisco powered device does not work on Cisco PoE switch. A non-Cisco powered device is connected to a Cisco PoE switch, but never powers on or powers on and then quickly powers off. Non-PoE devices work normally.	Use the **show power inline** command to verify that the switch power budget (available PoE) is not depleted before or after the powered device is connected. Verify that sufficient power is available for the powered device type before you connect it. Use the **show interface status** command to verify that the switch detects the connected powered device. Use the **show log** command to review system messages that reported an overcurrent condition on the port. Identify the symptom precisely: Does the powered device initially power on, but then disconnect? If so, the problem might be an initial surge-in (or *inrush*) current that exceeds a current-limit threshold for the port.

Configuration Examples for Troubleshooting Software

Example: Pinging an IP Host

This example shows how to ping an IP host:

```
Switch# ping 172.20.52.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Switch#
```

Table 5: Ping Output Display Characters

Character	Description
!	Each exclamation point means receipt of a reply.
.	Each period means the network server timed out while waiting for a reply.
U	A destination unreachable error PDU was received.
C	A congestion experienced packet was received.
I	User interrupted test.
?	Unknown packet type.
&	Packet lifetime exceeded.

To end a ping session, enter the escape sequence (**Ctrl-^ X** by default). Simultaneously press and release the **Ctrl**, **Shift**, and **6** keys and then press the **X** key.

Example: Performing a Traceroute to an IP Host

This example shows how to perform a **traceroute** to an IP host:

```
Switch# traceroute ip 192.0.2.10

Type escape sequence to abort.
Tracing the route to 192.0.2.10

  1 192.0.2.1 0 msec 0 msec 4 msec
  2 192.0.2.203 12 msec 8 msec 0 msec
  3 192.0.2.100 4 msec 0 msec 0 msec
  4 192.0.2.10 0 msec 4 msec 0 msec
```

The display shows the hop count, the IP address of the router, and the round-trip time in milliseconds for each of the three probes that are sent.

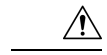
Table 6: Traceroute Output Display Characters

Character	Description
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this output means that an access list is blocking traffic.
H	Host unreachable.
N	Network unreachable.

Character	Description
P	Protocol unreachable.
Q	Source quench.
U	Port unreachable.

To end a trace in progress, enter the escape sequence (**Ctrl-^ X** by default). Simultaneously press and release the **Ctrl**, **Shift**, and **6** keys and then press the **X** key.

Example: Enabling All System Diagnostics



Caution Because debugging output takes priority over other network traffic, and because the **debug all** privileged EXEC command generates more output than any other **debug** command, it can severely diminish switch performance or even render it unusable. In virtually all cases, it is best to use more specific **debug** commands.

This command disables all-system diagnostics:

```
Switch# debug all
```

The **no debug all** privileged EXEC command disables all diagnostic output. Using the **no debug all** command is a convenient way to ensure that you have not accidentally left any **debug** commands enabled.

Additional References for Troubleshooting Software Configuration

Related Documents

Related Topic	Document Title
System management commands	
Platform-independent command reference	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*
Platform_independent configuration information	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support