



Troubleshooting

This chapter describes how to identify and resolve software problems related to the Cisco IOS software on the Catalyst 3750 switch. Depending on the nature of the problem, you can use the command-line interface (CLI) or the Cluster Management Suite (CMS) to identify and solve problems.

Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.

Additional troubleshooting information is provided in the hardware installation guide.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the command reference for this release and the *Cisco IOS Command Summary for Release 12.1*.

This chapter consists of these sections:

- [Recovering from Corrupted Software By Using the XMODEM Protocol, page 31-2](#)
- [Recovering from a Lost or Forgotten Password, page 31-4](#)
- [Recovering from Switch Stack Problems, page 31-8](#)
- [Recovering from a Command Switch Failure, page 31-9](#)
- [Recovering from Lost Cluster Member Connectivity, page 31-12](#)



Note Recovery procedures require that you have physical access to the switch.

- [Preventing Autonegotiation Mismatches, page 31-13](#)
- [Using the SDM Templates, page 31-13](#)
- [SFP Module Security and Identification, page 31-15](#)
- [Diagnosing Connectivity Problems, page 31-16](#)
- [Using Debug Commands, page 31-19](#)
- [Using the show platform forward Command, page 31-21](#)
- [Using the crashinfo File, page 31-23](#)

Recovering from Corrupted Software By Using the XMODEM Protocol

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 you are using.

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

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, refer to the release notes.

Step 2 Extract the bin file from the tar file.

- If you are using Windows, use a zip program that is capable of reading a tar file. Use the zip program to navigate to and extract the bin file.
- If you are using UNIX, follow these steps:
 1. Display the contents of the tar file by using the **tar -tvf <image_filename.tar>** UNIX command.

```
switch% tar -tvf image_filename.tar
drwxr-xr-x 9658/25      0 Apr 21 13:20 2003 c3750-i5-mz.121.11-AX/
drwxr-xr-x 9658/25      0 Apr 18 18:31 2003 c3750-i5-mz.121.11-AX/html/
-rw-r--r-- 9658/25     4005 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/homepage.htm
-rw-r--r-- 9658/25     1392 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/not_supported.html
-rw-r--r-- 9658/25     9448 Apr 18 15:56 2003 c3750-i5-mz.121.11-AX/html/common.js
-rw-r--r-- 9658/25    22152 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/cms_splash.gif
-rw-r--r-- 9658/25     1211 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/cms_13.html
-rw-r--r-- 9658/25     2823 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/cluster.html
-rw-r--r-- 9658/25     4195 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/Redirect.jar
-rw-r--r-- 9658/25    14984 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/mono_disc.sgz
-rw-r--r-- 9658/25   1329516 Apr 18 15:56 2003 c3750-i5-mz.121.11-AX/html/CMS.sgz
-rw-r--r-- 9658/25   140105 Apr 18 15:56 2003 c3750-i5-mz.121.11-AX/html/images.sgz
-rw-r--r-- 9658/25   213848 Apr 18 15:56 2003 c3750-i5-mz.121.11-AX/html/help.sgz
-rw-r--r-- 9658/25   135599 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/CiscoChartPanel.sgz
-rwxr-xr-x 9658/25     58860 Apr 18 18:31 2003
c3750-i5-mz.121.11-AX/html/cms_boot.jar
-rw-r--r-- 9658/25   3970586 Apr 21 12:00 2003
c3750-i5-mz.121.11-AX/c3750-i5-mz.121.11-AX.bin
-rw-r--r-- 9658/25      391 Apr 21 13:20 2003 c3750-i5-mz.121.11-AX/info
-rw-r--r-- 9658/25      98 Apr 18 16:46 2003 info
```

2. 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 c3750-i5-mz.121.11-AX/c3750-i5-mz.121.11-AX.bin, 3970586 bytes, 7756 tape blocks
```

3. Verify that the bin file was extracted by using the `ls -l <image_filename.bin>` UNIX command.

```
switch% ls -l image_filename.bin
-rw-r--r--  1 boba      3970586 Apr 21 12:00
c3750-i5-mz.121.11-AX/c3750-i5-mz.121.11-AX.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 along 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 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 or to the switch stack.

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.



Note

On these switches, 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.

This section describes how to recover a forgotten or lost switch password. It also provides two other solutions:

- [Procedure with Password Recovery Enabled, page 31-5](#)
- [Procedure with Password Recovery Disabled, page 31-6](#)

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

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

-
- Step 1** Connect a terminal or PC with terminal-emulation software to the switch console port. If you are recovering the password to a switch stack, connect to the console port of the stack master.
- Step 2** Set the line speed on the emulation software to 9600 baud.
- Step 3** Power off the standalone switch or the entire switch stack.
- Step 4** Press the **Mode** button, and at the same time, reconnect the power cord to the standalone switch or the stack master.

You can release the **Mode** button a second or two after the LED above port 1 turns off. Several lines of information about the software appear with instructions, informing you if the password recovery procedure has been disabled or not.

- If you see a message that begins with this:

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

proceed to the [“Procedure with Password Recovery Enabled” section on page 31-5](#), and follow the steps.

- If you see a message that begins with this:

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

proceed to the [“Procedure with Password Recovery Disabled” section on page 31-6](#), and follow the steps.

- Step 5** After recovering the password, reload the standalone switch or the stack master:

```
Switch> reload slot <stack-master-member-number>
Proceed with reload? [confirm] y
```

- Step 6** Power on the rest of the switch stack.
-

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
```

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  c3750-i5-mz-121-1.0
 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 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.

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
```

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 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 Elect to continue with password recovery and lose the existing configuration:

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

Step 2 Load any helper files:

```
Switch: load_helper
```

Step 3 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 c3750-i5-mz-121-1.0

16128000 bytes total (10003456 bytes free)
```

Step 4 Boot 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 5 At the switch prompt, enter privileged EXEC mode:

```
Switch> enable
```

Step 6 Enter global configuration mode:

```
Switch# configure terminal
```

Step 7 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 8 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 9 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 10 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 Switch Stack Problems



Note

- Make sure the switches that you add to or remove from the switch stack are powered off. For all powering considerations in switch stacks, refer to the “Switch Installation” chapter in the hardware installation guide.
- After adding or removing stack members, make sure that the switch stack is operating at full bandwidth (32 Gbps). Press the Mode button on a stack member until the Stack mode LED is on. The last two port LEDs on the switch should be green. Depending on the switch model, the last two ports are either 10/100/1000 ports or SFP module ports. If one or both of the last two port LEDs are not green, the stack is not operating at full bandwidth.
- We recommend using only one CLI session when managing the switch stack. Be careful when using multiple CLI sessions to the stack master. Commands you enter in one session are not displayed in the other sessions. Therefore, it is possible that you might not be able to identify the session from which you entered a command.
- Manually assigning stack member numbers according to the placement of the switches in the stack can make it easier to remotely troubleshoot the switch stack. However, you will need to remember that the switches have manually assigned numbers if you add, remove, or rearrange switches later. Use the **switch *current-stack-member-number* renumber *new-stack-member-number*** global configuration command to manually assign a stack member number. For more information about stack member numbers, see the “[Stack Member Numbers](#)” section on page 5-6.

If you replace a stack member with an identical model, the new switch functions with the exact same configuration as the replaced switch. This is also assuming the new switch is using the same member number as the replaced switch.

Removing powered-on stack members causes the switch stack to divide (partition) into two or more switch stacks, each with the same configuration. If you want the switch stacks to remain separate, change the IP address of the newly created switch stacks. To recover from a partitioned switch stack:

1. Power off the newly created switch stacks.
2. Reconnect them to the original switch stack through their StackWise ports.
3. Power on the switches.

For the commands you can use to monitor the switch stack and its members, see the “[Displaying Information about the Switch Stack](#)” section on page 5-14.

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). For more information, see [Chapter 6, “Clustering Switches”](#) and [Chapter 27, “Configuring 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 switches is lost, and you must install a new command switch. However, connectivity between switches that are still connected is not affected, and the member switches forward packets as usual. You can manage the members as standalone switches 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 switches and the replacement command switch. This section describes two solutions for replacing a failed command switch:

- [Replacing a Failed Command Switch with a Cluster Member, page 31-9](#)
- [Replacing a Failed Command Switch with Another Switch, page 31-11](#)

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

For information on command-capable switches, refer to 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:

-
- Step 1** Disconnect the command switch from the member switches, 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, refer to 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]:
```

**Step 10** Enter **Y** at the first prompt.

The prompts in the setup program vary depending on the member 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 11** Respond to the questions in the setup program.

When prompted for the host name, recall that on a command switch, the host name 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 host name 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 switches 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:

**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, refer to the switch hardware installation 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]:
```

**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 host name, recall that on a command switch, the host name is limited to 28 characters. Do not use *-n*, where *n* is a number, as the last characters in a host name 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 switches to add to the cluster.
- 

## Recovering from Lost Cluster Member Connectivity

Some configurations can prevent the command switch from maintaining contact with member switches. 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 3550, Catalyst 3500 XL, 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 switches must connect to the command switch through a port that belongs to the same management VLAN.
- A member switch (Catalyst 3750, Catalyst 3550, 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 Mbps, 100 Mbps, and 1000 Mbps, excluding SFP 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.

## Using the SDM Templates

You can use the Switch Database Management (SDM) templates to configure system resources in the switch to optimize support for specific features, depending on how the switch is used in the network. You can select a template to provide maximum system utilization for unicast routing or for VLAN configuration or use the default template to balance resources.

The templates prioritize system memory to optimize support for these types of features:

- Routing—The routing template maximizes system resources for unicast routing, typically required for a router or aggregator in the center of a network.
- VLANs—The VLAN template disables routing and supports the maximum number of unicast MAC addresses. It would typically be selected for a Layer 2 switch.
- Default—The default template gives balance to all functions.

Table 31-1 lists the approximate number of each resource supported in each of the three templates.

**Table 31-1** Approximate Number of Feature Resources Allowed by Each Template

| Resource                         | Default Template | Routing Template | VLAN Template |
|----------------------------------|------------------|------------------|---------------|
| Unicast MAC addresses            | 6 K              | 3 K              | 12 K          |
| IGMP groups and multicast routes | 1 K              | 1 K              | 1 K           |
| Unicast routes                   | 8 K              | 11 K             | 0             |
| • Directly connected hosts       | 6 K              | 3 K              | 0             |
| • Indirect routes                | 2 K              | 8 K              | 0             |
| QoS classification ACEs          | 512              | 512              | 512           |
| Security ACEs                    | 1 K              | 1 K              | 1 K           |

**Table 31-1** Approximate Number of Feature Resources Allowed by Each Template (continued)

| Resource                                  | Default Template | Routing Template | VLAN Template |
|-------------------------------------------|------------------|------------------|---------------|
| Routed interfaces (routed ports and SVIs) | 8                | 8                | 8             |
| Layer 2 VLANs                             | 1 K              | 1 K              | 1 K           |

The first seven rows in the tables (unicast MAC addresses through security ACEs) represent approximate hardware boundaries set when a template is selected. If a section of a hardware resource is full, all processing overflow is sent to the CPU, seriously impacting switch performance.

The last two rows, the total number of routed ports and SVIs and the number of Layer 2 VLANs, are guidelines used to calculate hardware resource consumption related to the other resource parameters.

The total number of routed interfaces is not limited by software and can be set to a number higher than shown in the tables. If the number of routed interfaces configured is lower or equal to the number in the tables, the number of entries in each category (unicast MAC addresses, IGMP groups, and so on) for each template will be as shown. As the number of routed interfaces is increased, CPU utilization typically increases. If the number of routed interfaces is increased beyond the number shown in the tables, the number of supported entries in each category could decrease depending on other features that are enabled.

Follow these guidelines when using the SDM templates:

- When you use the VLAN template, no system resources are reserved for routing entries and any routing is done through software. This overloads the central processing unit (CPU) and severely degrades routing performance. Use the **sdm prefer vlan** global configuration command only on switches intended for Layer 2 switching with no routing.
- Do not use the routing template if you do not have routing enabled on your switch. Entering the **sdm prefer routing** global configuration command prevents other features from using the hardware resources allocated to unicast routing in the routing template (approximately 11 K).
- The switch must reload for the configuration to take effect. If you use the **show sdm prefer** privileged EXEC command before the switch reloads, the previous configuration is displayed.

All stack members use the same SDM template, stored on the stack master. When a new switch member is added to a stack, as with the switch configuration file and VLAN database file, the SDM configuration that is stored on the stack master overrides the template configured on an individual switch.

Beginning in privileged EXEC mode, follow these steps to use the SDM template to maximize feature usage:

|        | Command                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>          | Enter global configuration mode.                                                                                                                                                                                                                                                                                                                                                                |
| Step 2 | <b>sdm prefer {routing   vlan}</b> | Specify the SDM template to be used on the switch:<br>The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>routing</b>—Maximizes routing on the switch.</li> <li>• <b>vlan</b>—Maximizes VLAN configuration on the switch with no routing allowed.</li> </ul> The default template (if neither of these is configured) balances system resources across all resources. |

|        | Command       | Purpose                         |
|--------|---------------|---------------------------------|
| Step 3 | <b>end</b>    | Return to privileged EXEC mode. |
| Step 4 | <b>reload</b> | Reload the operating system.    |

After the system reboots, you can use the **show sdm prefer** privileged EXEC command to verify the new template configuration. If you use the **show sdm prefer** command before the **reload** privileged EXEC command, the previous template is displayed instead of the new one. To return to the default template, use the **no sdm prefer** global configuration command.

**Note**

Use the **show sdm prefer {default | routing | vlan}** privileged EXEC command to display the resource numbers supported by the specified template. Use the **show sdm prefer** privileged EXEC command with no parameters to display the active template.

This example shows how to configure a switch with the routing template and verify the configuration:

```
Switch(config)# sdm prefer routing
Switch(config)# end
Switch# reload
Proceed with reload? [confirm]
```

## SFP Module Security and Identification

Cisco-approved 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 Catalyst 3750 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 interfaces and modules. For more information about error messages, refer to the system message guide for this release.

If you are using a non-Cisco approved SFP module, remove the SFP from the switch, and replace it with a Cisco-approved module. After inserting a Cisco-approved 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, refer to the command reference for this release.

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

# Diagnosing Connectivity Problems

This section describes how to troubleshoot connectivity problems:

- [Understanding Ping, page 31-16](#)
- [Executing Ping, page 31-16](#)
- [Understanding IP Traceroute, page 31-17](#)
- [Executing IP Traceroute, page 31-18](#)

## Understanding 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. For more information, see [Chapter 26, “Configuring IP Unicast Routing.”](#)

IP routing is disabled by default on all switches. If you need to enable or configure IP routing, see [Chapter 26, “Configuring IP Unicast Routing.”](#)

Beginning in privileged EXEC mode, use this command to ping another device on the network from the switch:

| Command                             | Purpose                                                                         |
|-------------------------------------|---------------------------------------------------------------------------------|
| <code>ping ip host   address</code> | Ping a remote host through IP or by supplying the host name or network address. |



### Note

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

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 31-2 describes the possible ping character output.

**Table 31-2 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 terminate a ping session, enter the escape sequence (**Ctrl-^ X** by default). You enter the default by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys, and then pressing the **X** key.

## Understanding 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 switches 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 switches 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 back an Internet Control Message Protocol (ICMP) time-to-live-exceeded message to the sender. Traceroute determines 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 determine 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 this message was sent by the destination.

## Executing IP Traceroute

Beginning in privileged EXEC mode, follow this step to trace the path packets take through the network:

| Command                         | Purpose                                                      |
|---------------------------------|--------------------------------------------------------------|
| <code>traceroute ip host</code> | Trace the path packets take through the network by using IP. |



### Note

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

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

```
Switch# traceroute ip 171.9.15.10

Type escape sequence to abort.
Tracing the route to 171.69.115.10

 0 172.2.52.1 0 msec 0 msec 4 msec
 1 172.2.1.203 12 msec 8 msec 0 msec
 2 171.9.16.6 4 msec 0 msec 0 msec
 3 171.9.4.5 0 msec 4 msec 0 msec
 4 171.9.121.34 0 msec 4 msec 4 msec
 5 171.9.15.9 120 msec 132 msec 128 msec
 6 171.9.15.10 132 msec 128 msec 128 msec
Switch#
```

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

**Table 31-3 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.                                                                              |
| P         | Protocol unreachable.                                                                             |
| Q         | Source quench.                                                                                    |
| U         | Port unreachable.                                                                                 |

To terminate a trace in progress, enter the escape sequence (**Ctrl-^ X** by default). You enter the default by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys, and then pressing the **X** key.

# Using Debug Commands

This section explains how you use **debug** commands to diagnose and resolve internetworking problems. It contains this information:

- [Enabling Debugging on a Specific Feature, page 31-19](#)
- [Enabling All-System Diagnostics, page 31-20](#)
- [Redirecting Debug and Error Message Output, page 31-20](#)

**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.

**Note**

For complete syntax and usage information for specific **debug** commands, refer to the command reference for this release.

## Enabling Debugging on a Specific Feature

When you enable debugging, it is enabled only on the stack master switch. To enable debugging on a stack member, you must start a session from the stack master by using the **session *switch-number*** privileged EXEC command. Then, enter the **debug** command at the command-line prompt of the stack member.

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
```



### 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.

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. Logging messages to the console produces very high overhead, whereas logging messages to a virtual terminal produces less overhead. Logging messages to a syslog server produces even less, and logging to an internal buffer produces the least overhead of any method.

When stack members generate a system error message, the stack master displays the error message to all stack members. The syslog resides on the stack master.



### Note

Make sure to save the syslog to Flash memory so that the syslog is not lost if the stack master fails.

For more information about system message logging, see [Chapter 21, “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, refer to 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.

This is an example of the output from the **show platform forward** command on Gigabit Ethernet port 24 on stack member 1 in VLAN 5 when the packet entering that port is addressed to unknown MAC addresses. The packet should be flooded to all other ports in VLAN 5.

```
Switch# show platform forward gigabitethernet1/0/24 vlan 5 1.1.1 2.2.2 ip 13.1.1.1
13.2.2.2 udp 10 20
```

```
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5
```

Ingress:

| Lookup                                            | Key-Used | Index-Hit | A-Data   |
|---------------------------------------------------|----------|-----------|----------|
| InptACL 40_0D020202_0D010101-00_40000014_000A0000 |          | 01FFA     | 03000000 |
| L2Local 80_00050002_00020002-00_00000000_00000000 |          | 00C71     | 0000002B |

Station Descriptor:02340000, DestIndex:0239, RewriteIndex:F005

```
=====
Egress:Asic 2, switch 1
```

Output Packets:

-----

Packet 1

| Lookup                                             | Key-Used | Index-Hit | A-Data   |
|----------------------------------------------------|----------|-----------|----------|
| OutptACL 50_0D020202_0D010101-00_40000014_000A0000 |          | 01FFE     | 03000000 |

| Port    | Vlan | SrcMac         | DstMac         | Cos | Dscp |
|---------|------|----------------|----------------|-----|------|
| Gi1/0/3 | 0005 | 0001.0001.0001 | 0002.0002.0002 |     |      |

-----

Packet 2

| Lookup                                             | Key-Used | Index-Hit | A-Data   |
|----------------------------------------------------|----------|-----------|----------|
| OutptACL 50_0D020202_0D010101-00_40000014_000A0000 |          | 01FFE     | 03000000 |

| Port    | Vlan | SrcMac         | DstMac         | Cos | Dscp |
|---------|------|----------------|----------------|-----|------|
| Gi1/0/4 | 0005 | 0001.0001.0001 | 0002.0002.0002 |     |      |

-----

Packet 3

| Lookup                                             | Key-Used | Index-Hit | A-Data   |
|----------------------------------------------------|----------|-----------|----------|
| OutptACL 50_0D020202_0D010101-00_40000014_000A0000 |          | 01FFE     | 03000000 |

| Port    | Vlan | SrcMac         | DstMac         | Cos | Dscp |
|---------|------|----------------|----------------|-----|------|
| Gi1/0/2 | 0005 | 0001.0001.0001 | 0002.0002.0002 |     |      |

-----

<output truncated>

```

Packet 10
 Lookup Key-Used Index-Hit A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000 01FFE 03000000
Packet dropped due to failed DEJA_VU Check on Gi1/0/24
```

This is an example of the output when the packet coming in on Gigabit Ethernet port 24 on stack member 1 in VLAN 5 is sent to an address already learned on the VLAN on another port. It should be forwarded from the port on which the address was learned.

```
Switch# show platform forward giigabitethernet1/0/24 vlan 5 1.1.1 0009.43a8.0145 ip
13.1.1.1 13.2.2.2 udp 10 20
```

```
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5
```

```
Ingress:
 Lookup Key-Used Index-Hit A-Data
InptACL 40_0D020202_0D010101-00_40000014_000A0000 01FFA 03000000
L2Local 80_00050009_43A80145-00_00000000_00000000 00086 02010197
Station Descriptor:F0050003, DestIndex:F005, RewriteIndex:0003
```

```
=====
Egress:Asic 3, switch 1
Output Packets:
```

```

Packet 1
 Lookup Key-Used Index-Hit A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000 01FFE 03000000
```

```
Port Vlan SrcMac DstMac Cos Dscpv
Gi1/0/5 0005 0001.0001.0001 0009.43A8.0145
```

This is an example of the output when the packet coming in on Gigabit Ethernet port 24 on stack member 1 in VLAN 5 has a destination MAC address set to the router MAC address in VLAN 5 and the destination IP address unknown. Since there is no default route set, the packet should be dropped.

```
Switch# show platform forward gigabitethernet1/0/24 vlan 5 1.1.1 03.e319.ee44 ip 13.1.1.1
13.2.2.2 udp 10 20
```

```
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5
```

```
Ingress:
 Lookup Key-Used Index-Hit A-Data
InptACL 40_0D020202_0D010101-00_41000014_000A0000 01FFA 03000000
L3Local 00_00000000_00000000-90_00001400_0D020202 010F0 01880290
L3Scndr 12_0D020202_0D010101-00_40000014_000A0000 034E0 000C001D_00000000
Lookup Used:Secondary
Station Descriptor:02260000, DestIndex:0226, RewriteIndex:0000
```

This is an example of the output when the packet coming in on Gigabit Ethernet port 24 on stack member 1 in VLAN 5 has a destination MAC address set to the router MAC address in VLAN 5 and the destination IP address set to an IP address that is in the IP routing table. It should be forwarded as specified in the routing table.

```
Switch# show platform forward gigabitethernet1/0/24 vlan 5 1.1.1 03.e319.ee44 ip 110.1.5.5
16.1.10.5
```

```
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5
```

```
Ingress:
 Lookup Key-Used Index-Hit A-Data
```

```

InptACL 40_10010A05_0A010505-00_41000014_000A0000 01FFA 03000000
L3Local 00_00000000_00000000-90_00001400_10010A05 010F0 01880290
L3Scndr 12_10010A05_0A010505-00_40000014_000A0000 01D28 30090001_00000000
Lookup Used:Secondary
Station Descriptor:F0070007, DestIndex:F007, RewriteIndex:0007

=====
Egress:Asic 3, switch 1
Output Packets:

Packet 1
Lookup Key-Used Index-Hit A-Data
OutptACL 50_10010A05_0A010505-00_40000014_000A0000 01FFE 03000000

Port Vlan SrcMac DstMac Cos Dscpv
Gi1/0/7 0007 XXXX.XXXX.0246 0009.43A8.0147

```

## Using the crashinfo File

The crashinfo file saves information that helps Cisco technical support representatives to debug problems that caused the IOS image to fail (crash). The switch writes the crash information to the console at the time of the failure, and the file is created the next time you boot the IOS image after the failure (instead of while the system is failing).

The information in the file includes the IOS image name and version that failed, a dump 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.

All crashinfo files are kept in this directory on the Flash file system:

flash:/crashinfo/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 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.

