CHAPTER 26

Troubleshooting

This chapter describes how to identify and resolve software problems related to the IOS software. 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. To identify and resolve Cisco-approved Course Wave Division Multiplexer (CWDM) Gigabit Interface Converter (GBIC) problems, you must have the enhanced software image installed on your switch.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 2950 Desktop Switch Command Reference* for this release and the *Cisco IOS Command Summary for Release 12.1*.

This chapter consists of these sections:

For additional troubleshooting information, refer to the switch hardware installation guide.

Avoiding Configuration Conflicts

Certain combinations of port features conflict with one another. For example, if you define a port as the network port for a VLAN, all unknown unicast and multicast traffic is flooded to the port. You could not enable port security on the network port because a secure port limits the traffic allowed on it.

In Table 26-1, *no* means that the two features are incompatible, and that both should not be enabled; *yes* means that both can be enabled at the same time and will not cause an incompatibility conflict.

If you try to enable incompatible features by using CMS, it issues a warning message that you are configuring a setting that is incompatible with another setting, and the switch does not save the change.

Table 26-1 Conflicting Features

	Port Group	Port Security	SPAN Source Port	SPAN Destination Port	Connect to Cluster?	Protected Port	802.1X Port
Port Group	–	No	Yes	No	Yes	Yes	No
Port Security	No	–	Yes	No	Yes	No	No
SPAN Source Port	Yes	Yes	–	No	Yes	Yes[1]	Yes
SPAN Destination Port	No	No	No	–	Yes	Yes	No
Connect to Cluster	Yes	Yes	Yes	Yes	–	Yes	–
Protected Port	Yes	No	Yes[1]	Yes[1]	Yes	–	–
802.1X Port	No	No	Yes	No	–	–	–

1. Switch Port Analyzer (SPAN) can operate only if the monitor port or the port being monitored is not a protected port.

Avoiding Autonegotiation Mismatches

The IEEE 802.3U autonegotiation protocol manages the switch settings for speed (10, 100, or 1000 Mbps) and duplex (half or full). Sometimes 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 Fast Ethernet 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. To connect to a remote Gigabit Ethernet device that does not autonegotiate, disable autonegotiation on the local device, and set the duplex and flow control parameters to be compatible with the remote device.

GBIC Security and Identification

Cisco-approved GBIC modules have a serial EEPROM that contains the module serial number, the vendor name and ID, a unique security code, and a cyclic redundancy check (CRC). When a GBIC module is inserted in the switch, the switch software reads the EEPROM to check the serial number, vendor name, and vendor ID, and recomputes the security code and CRC. If the serial number, the vendor name or ID, the security code, or CRC is invalid, the switch places the interface in an error-disabled state.

Note If you are using a non-Cisco approved GBIC module, remove the GBIC module from the switch, and replace with a Cisco-approved module.

After inserting a Cisco-approved GBIC, 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 *Catalyst 2950 Desktop Switch Command Reference.*

Troubleshooting CMS Sessions

Table 26-2 lists problems commonly encountered when using CMS:

Table 26-2 Common CMS Session Problems

Problem	Suggested Solution
A blank screen appears when you click **Web Console** from the CMS access page.	A missing Java plug-in or incorrect settings could cause this problem. • CMS requires a Java plug-in order to function correctly. For instructions on downloading and installing the plug-ins, refer to the *Release Notes for the Catalyst 2950* for this release. **Note** If your PC is connected to the Internet when you attempt to access CMS, the browser notifies you that the Java plug-in is required if the Java plug-in is not installed. This notification does not occur if your PC is directly connected to the switch and has no Internet connection. • If the plug-in is installed but the Java applet does not initialize, do this: – Select **Start > Programs > Java Plug-in Control Panel**. Click the **Proxies** tab, and verify that **Use browser settings** is checked and that no proxies are enabled. – Make sure that the HTTP port number is 80. CMS only works with port 80, which is the default HTTP port number. – Make sure the port that connects the PC to the switch belongs to the same VLAN as the management VLAN. For more information about management VLANs, see the "Management VLANs" section on page 13-3.

Table 26-2 Common CMS Session Problems (continued)

Problem	Suggested Solution
The **Applet notinited** message appears at the bottom of the browser window.	You might not have enough disk space. Each time you start CMS, Java Plug-in 1.2.2 saves a copy of all the jar files to the disk. Delete the jar files from the location where the browser keeps the temporary files on your computer.
In an Internet Explorer browser session, you receive a message stating that the CMS page might not display correctly because your security settings prohibit running ActiveX controls.	A high security level prohibits ActiveX controls (which Internet Explorer uses to launch the Java plug-in) from running. Do this: 1. Start Internet Explorer. 2. From the menu bar, select **Tools > Internet Options**. 3. Click the **Security** tab. 4. Click the indicated **Zone**. 5. Move the **Security Level for this Zone** slider from **High** to **Medium** (the default). 6. Click **Custom Level...** and verify that these ActiveX controls and plug-ins are set to either **Prompt** or **Enable**: • Download signed ActiveX controls. • Download unsigned ActiveX controls as safe. • Initialize and script ActiveX controls not marked. • Run ActiveX controls and plug-ins.

For further debugging information, you can use the Java plug-ins Java console to display the current status and actions of CMS. To display the Java console, select **Start > Programs > Java Plug-in Control Panel**, and select **Show Java Console**.

Copying Configuration Files to Troubleshoot Configuration Problems

You can use the file system in Flash memory to copy files and to troubleshoot configuration problems. This could be useful if you want to save configuration files on an external server in case a switch fails. You can then copy the configuration file to a replacement switch and avoid reconfiguring the switch.

Step 1 Enter the **dir flash:** privileged EXEC command to display the contents of Flash memory as in this example:

```
switch: dir flash:
```

The switch file system appears:

```
Directory of flash:/
  3  drwx       10176   Mar 01 2001 00:04:34  html
  6  -rwx        2343   Mar 01 2001 03:18:16  config.text
171  -rwx     1667997   Mar 01 2001 00:02:39  c2950-i6q412-mz.121-9.EA1.bin
  7  -rwx        3060   Mar 01 2001 00:14:20  vlan.dat
172  -rwx         100   Mar 01 2001 00:02:54  env_vars

7741440 bytes total (3884509 bytes free)
```

The file system uses a URL-based file specification. This example uses the TFTP protocol to copy the file config.text from the host *arno* to the switch Flash memory:

```
switch# copy tftp://arno//2950/config.text flash:config.text
```

You can enter these parameters as part of a filename:

- TFTP
- Flash
- RCP
- XMODEM

Step 2 Enter the **copy running-config startup-config** privileged EXEC command to save your configuration changes to Flash memory so that they are not lost if there is a system reload or power outage. This example shows how to use this command to save your changes:

```
switch# copy running-config startup-config
Building configuration...
```

It might take a minute or two to save the configuration to Flash memory. After it has been saved, this message appears:

```
[OK]
switch#
```

Using Recovery Procedures

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

- Recovering from lost member connectivity
- Recovering from a command-switch failure
- Recovering from a lost or forgotten password
- Recovering from corrupted software

Recovering from Lost 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 port-configuration conflicts:

- Member switches cannot connect to the command switch through a port that is defined as a network port.
- Member switches must connect to the command switch through a port that belongs to the same management VLAN. For more information, see the "Management VLAN" section on page 6-20.
- Member switches connected to the command switch through a secure port can lose connectivity if the port is disabled due to a security violation. Secure ports are described in the "Configuring Port Security" section on page 17-3.

Recovering from a Command Switch Failure

You can prepare for a command switch failure by assigning an IP address to a member switch that is command-capable, making a note of the command-switch password, and cabling your cluster to provide redundant connectivity between all member switches and the replacement command switch. Hot Standby Router Protocol (HSRP) is the preferred method for providing a redundant command switch to a cluster. For more information, see the "HSRP and Standby Command Switches" section on page 6-14 and the "Creating a Cluster Standby Group" section on page 6-25. For a list of command-capable Catalyst switches, refer to the *Release Notes for the Catalyst 2950 Switch* on Cisco.com.

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 a new command switch must be installed. 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 CMS Device Manager.

These sections describe how to recover if a standby command switch was not available when the command switch failed:

- "Replacing a Failed Command Switch with a Cluster Member" section on page 26-6
- "Replacing a Failed Command Switch with Another Switch" section on page 26-8
- "Recovering from a Failed Command Switch Without HSRP" section on page 26-9

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 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 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, 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 appears, 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 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 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, 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 appears, 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.

From the Cluster menu, select **Add to Cluster** to display a list of candidate switches to add to the cluster.

Recovering from a Failed Command Switch Without HSRP

If a command switch fails and there is no standby command switch configured, member switches continue forwarding among themselves, and they can still be managed through normal standalone means. You can configure member switches through the console-port CLI, and they can be managed through SNMP, HTML, and Telnet after you assign an IP address to them.

The password that you enter when you log in to the command switch gives you access to member switches. If the command switch fails and there is no standby command switch, you can use the command-switch password to recover. For more information, see the "Recovering from a Command Switch Failure" section on page 26-6.

Recovering from a Lost or Forgotten Password

Follow these steps if you have forgotten or lost the switch password.

Step 1 Connect a terminal or PC with terminal emulation software to the console port. For more information, refer to the switch hardware installation guide.

Note You can configure your switch for Telnet by following the procedure in the "Accessing the CLI" section on page 2-9.

Step 2 Set the line speed on the emulation software to 9600 baud.

Step 3 Unplug the switch power cord.

Step 4 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 1X goes off. Several lines of information about the software appear, as do instructions:

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

flash_init
load_helper
boot
```

Step 5 Initialize the Flash file system:

```
switch: flash_init
```

Step 6 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 7 Load any helper files:

```
switch: load_helper
```

Step 8 Display the contents of Flash memory as in this example:

```
switch: dir flash:
The switch file system is displayed:
Directory of flash:/
  3  drwx       10176   Mar 01 2001 00:04:34  html
  6  -rwx        2343   Mar 01 2001 03:18:16  config.text
171  -rwx     1667997   Mar 01 2001 00:02:39  c2950-i6q412-mz.121-9.EA1.bin
  7  -rwx        3060   Mar 01 2001 00:14:20  vlan.dat
172  -rwx         100   Mar 01 2001 00:02:54  env_vars

7741440 bytes total (3884509 bytes free)
```

Step 9 Rename the configuration file to config.text.old.

This file contains the password definition.

```
switch: rename flash:config.text flash:config.text.old
```

Step 10 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 11 At the switch prompt, change to privileged EXEC mode:

```
switch> enable
```

Step 12 Rename the configuration file to its original name:

```
switch# rename flash:config.text.old flash:config.text
```

Step 13 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 use the following normal commands to change the password.

Step 14 Enter global configuration mode:

```
switch# config terminal
```

Step 15 Change the password:

```
switch(config)# enable secret <password>
```

or

```
switch(config)# enable password <password>
```

Step 16 Return to privileged EXEC mode:

```
switch(config)# exit
switch#
```

Step 17 Write the running configuration to the startup configuration file:

```
switch# copy running-config startup-config
```

The new password is now included in the startup configuration.

Recovering from Corrupted Software

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

The 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.

Step 1 Connect a PC with terminal-emulation software supporting the XMODEM Protocol to the switch console port.

Step 2 Set the line speed on the emulation software to 9600 baud.

Step 3 Disconnect the switch power cord.

Step 4 Reconnect the power cord to the switch.

The software image does not load. The switch starts in boot loader mode, which is indicated by the `switch:` prompt.

Step 5 Use the boot loader to enter commands, and start the transfer.

```
switch: copy xmodem: flash:image_filename.bin
```

Step 6 When the XMODEM request appears, use the appropriate command on the terminal-emulation software to start the transfer and to copy the software image to Flash memory.

Using Debug Commands

This section explains how you use **debug** commands to diagnose and resolve internetworking problems:

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.

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 EtherChannel:

```
Switch# debug etherchannel
```

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 when 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 EtherChannel, enter this command in privileged EXEC mode:

```
Switch# no debug etherchannel
```

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

```
Switch# undebug etherchannel
```

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** 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** 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 that 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.