CHAPTER 9

Troubleshooting

This chapter provides the following information about avoiding and resolving problems related to the switch software.

- Avoiding configuration conflicts
- Avoiding autonegotiation mismatches
- Copying configuration files to troubleshooting configuration problems
- Troubleshooting the Long-Reach Ethernet port configuration
- Troubleshooting Cluster Management Suite (CMS) sessions
- Troubleshooting switch upgrades
- Recovering from corrupted software
- Recovering from a lost or forgotten password

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 9-1, *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, CMS 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 9-1 Conflicting Features

	ATM Port[1]	Port Group	Port Security	SPAN Port	Multi-VLAN Port	Network Port	Connect to Cluster?	Protected Port
ATM Port	N/A	No	No	No	No	No	Yes	No
Port Group	No	–	No	No	Yes	Yes[2]	Yes	Yes
Port Security	No	No	–	No	No	No	Yes	Yes
SPAN Port	No[3]	No	No	–	No	No	Yes	Yes
Multi-VLAN Port	No	Yes	No	No	–	Yes	Yes	Yes
Network Port	No	Yes (source-based only)	No	No	Yes	–	No[4]	Yes
Connect to Cluster	Yes	Yes	Yes	Yes	Yes	No	–	Yes
Protected Port	No	Yes	Yes	Yes[5]	Yes	No	Yes	–

1. Catalyst 2900 XL switches only.
2. Cannot be in a destination-based port group.
3. An Asynchronous Transfer Mode (ATM) port cannot be a monitor port but can be monitored.
4. Cannot connect cluster members to the command switch.
5. 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 Mbps or 100 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.

Troubleshooting LRE Port Configuration

Table 9-2 lists problems you might encounter when configuring and monitoring the Long-Reach Ethernet (LRE) ports on the Catalyst 2900 LRE XL switches.

Table 9-2 LRE Port Problems

Problem	Suggested Solution
LRE port LED is amber	The switch and CPE are unable to establish a LRE link using the selected profile. Change to a profile using a lower quadrature amplitude modulation (QAM) rate. Reduce the effect of stubs or bridge taps by terminating them with 300-Ohm microfilters.
Excessive CRC errors on a LRE link	• A noisy environment (such as motors and power surges) is causing interference with the LRE link. Ensure that the interleaver is set to maximum protection (the interleaver trades latency for noise immunity). Change to a profile using a lower QAM rate, which increases the noise margin. • The LRE link length and quality are close to the limit of operation. Change to a profile using a lower QAM rate. Reduce the effect of stubs or bridge taps by terminating them with 300-Ohm microfilters.
High Reed-Solomon error count without CRC errors	• Interleaver is helping Reed-Solomon error correction to function correctly in a noisy environment. This situation means that the system is on the verge of generating CRC errors. Ensure that the interleaver is set to maximum protection (the interleaver trades latency for noise immunity). Change to a profile using a lower QAM rate, which increases the noise margin. • The LRE link length and quality are close to the limit of operation. Change to a profile using a lower QAM rate. Reduce the effect of stubs or bridge taps by terminating them with 300-Ohm microfilters.
Ethernet performance degradation due to excessive network latency	Interleaver introduces extra latency to increase noise margin. Reduce the interleaver setting while ensuring the noise margin is adequate. If necessary, change to a profile using a lower QAM rate.
LRE link quality reduced in installations with bundled cables	Cross-talk between the LRE links is causing all links to degrade. Disable unused LRE ports by using the **lre shutdown** interface configuration command.

Troubleshooting CMS Sessions

Table 9-3 lists problems commonly encountered when using CMS:

Table 9-3 Common CMS Session Problems

Problem	Suggested Solution
A blank screen appears when you click **Cluster Management Suite or Visual Switch Manager** from the Cisco Systems Access page.	A missing browser Java plug-in or incorrect settings could cause this problem. • CMS requires a Java plug-in to function correctly. For instructions on downloading and installing the plug-in, refer to the release notes. **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 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 the following: – Select **Start > Programs > Java Plug-in Control Panel**. In the **Proxies** tab, 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 8-4.
The **Applet notinited** message appears at the bottom of the browser window.	You might not have enough disk space. Each time you start CMS, the Java plug-in 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. Refer to the release notes for the required Java plug-ins.

Table 9-3 Common CMS Session Problems (continued)

Problem	Suggested Solution
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. 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 the four ActiveX settings are set to **prompt** or **enabled**.
Configuration changes are not always reflected in an Internet Explorer 5.0 browser session.	Microsoft Internet Explorer 5.0 does not automatically reflect the latest configuration changes. Make sure you click the browser **Refresh** button for every configuration change.
Link graphs do not display information in an Internet Explorer 5.0 browser. (For switches running software earlier than Cisco IOS Release 12.0(5)WC(1).)	Your browser security settings could be incorrect. If your browser security settings are correct, the lower right corner of your browser screen should have a green circle with a checkmark. If it does not, follow these steps: 1. Start Internet Explorer. 2. From the menu bar, select **Tools > Internet Options**. 3. From the Internet Options window, click **Advanced**. 4. Select the **Java logging enabled** and **JIT compiler for virtual machine enabled** check boxes, and click **Apply**. 5. In the Internet Options window, click **General**. 6. In the Temporary Internet Files section, click **Settings**, click **Every visit to the page**, and click **OK**. 7. In the Internet Options window, click **Security**, click **Trusted Sites**, and click **Sites**. 8. Deselect **Require server verification**.

Table 9-3 Common CMS Session Problems (continued)

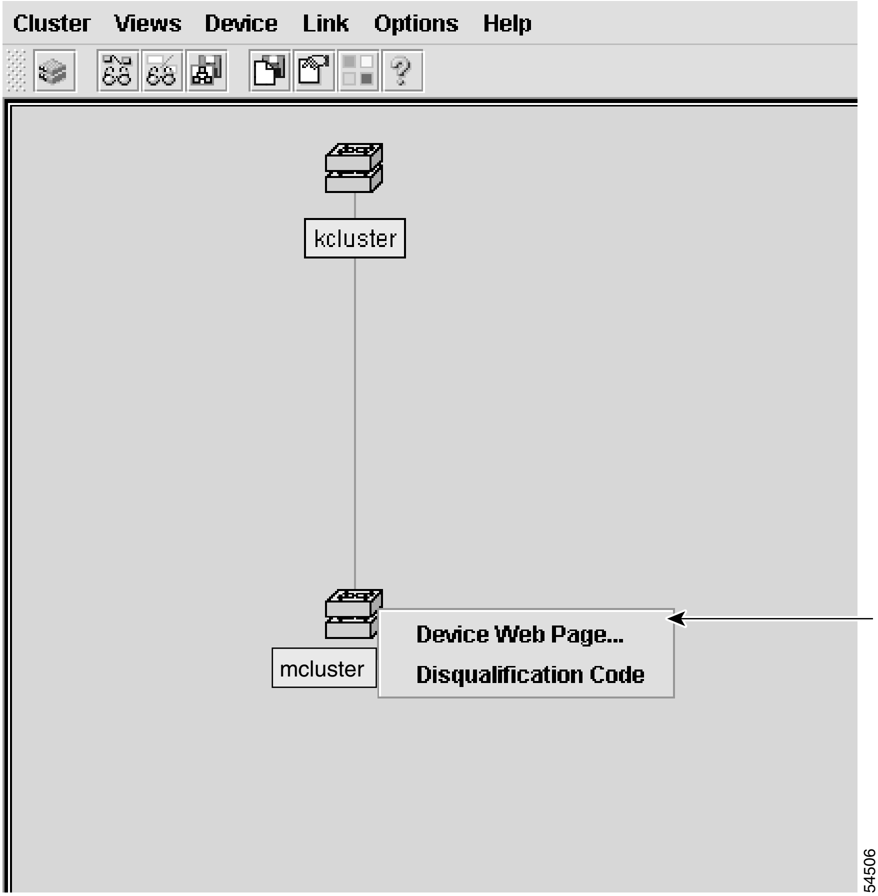
Problem	Suggested Solution
	9. Add the switches you want to manage by entering their URLs in the **Add this web site to the zone** field. Click **Add** to add each switch. A URL is the switch IP address preceded by http://. For example, you might enter: `http://172.20.153.36` 10. After you have finished entering the URLs for your switches, click **OK**. 11. While still in the **Security** tab of the Internet Options window, click **Custom Level**. 12. In the Security Settings window, select **Java > Java permissions**. If you do not see **Java > Java permissions**, you need to reinstall the browser. When you reinstall this browser, make sure to select the **Install Minimal or Customize Your Browser** check box. Then, from the Component Options window in the Internet Explorer 5 section, make sure to click the **Microsoft Virtual Machine** check box to display applets written in Java. 13. Click **Custom**, and click **Java Custom Settings**. 14. In the Trusted Sites window, click **Edit Permissions**. 15. Under **Run Unsigned Content**, click **Enable**, and click **OK**. 16. In the Security Settings window, click **OK**. 17. In the Internet Options window, click **OK**.

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

Determining Why a Switch Is Not Added to a Cluster

If a switch does not become part of the cluster, you can learn why by selecting **Views > Toggle View** from the menu bar in Cluster Builder. Cluster View displays the cluster as a double-switch icon and shows connections to devices outside the cluster (Figure 9-1). Right-click the device (yellow label), and select **Disqualification Code**.

Figure 9-1 Cluster View



Right-click a device with a yellow label to display the device pop-up menu, and select **Disqualification Code** to display the reason it could not join the cluster.

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 wanted 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 having to reconfigure the switch.

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

```
switch# dir flash:
Directory of flash:

  2  -rwx      843947   Mar 01 1993 00:02:18  C2900XL-h-mz-112.8-SA
  4  drwx        3776   Mar 01 1993 01:23:24  html
 66  -rwx         130   Jan 01 1970 00:01:19  env_vars
 68  -rwx        1296   Mar 01 1993 06:55:51  config.text

1728000 bytes total (456704 bytes free)
```

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

```
switch# copy tftp://arno//2900/config.text flash:config.text
```

You can enter the following 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, the following message appears:

```
[OK]
switch#
```

Troubleshooting Switch Upgrades

Table 9-4 lists problems commonly encountered when upgrading the switch:

Table 9-4 Problems Encountered When Upgrading the Switch

Problem	Suggested Solution
Getting "Address Range" error message and boot up is failing.	This error message appears when a 4-MB Catalyst 2900 XL switch is upgraded to an image that is not supported on this hardware. The switch in this case tries to load the image, but because this switch is not capable of loading this image, the bootup process fails. This also happens in cases when a 4-MB Catalyst 2900 XL switch is upgraded to an IOS 12.0 image. Download the IOS Image File by using X-Modem.
Getting "No Such File or Directory" error message during bootup.	This error message appears when the names of the bootable file and the actual file in the Flash differ. This usually happens due to a mistyped file name when setting the boot parameters, during or after the upgrade. Go to Setting BOOT Parameters at ROMMON (Switch: Prompt) to verify and set the BOOT parameters correctly. If setting the BOOT parameters to the correct file name does not resolve the issue, perform an X-Modem upgrade, as the file present on the Flash memory could be corrupted or invalid.

Table 9-4 Problems Encountered When Upgrading the Switch (continued)

Problem	Suggested Solution
Getting “Permission Denied” error message during the bootup.	This error message appears when the boot parameters are not set correctly. In most of the cases, when setting the boot parameters during or after the upgrade, the word flash: is mistyped or completely missed. Go to Setting BOOT Parameters at ROMMON (Switch: Prompt) to verify and set the BOOT parameters correctly. If setting the BOOT parameters to the correct file name does not resolve the issue, perform an X-Modem upgrade, as the file present on the Flash memory could be corrupted or invalid.
Getting “Error Loading Flash” error messages.	The error loading Flash message means that there is a problem loading the current image in Flash memory. The image could be corrupt or incorrect, or the image in Flash memory could be missing. If the system is unable to load a software image in Flash memory, the system will load the boot helper and bring up a switch prompt. 1. Enter the **dir flash:** command to verify if there is any bootable image on the Flash. The file with .bin extension is the bootable image on the Flash. If you see a bootable image on the Flash, continue to Step 2. If you do not see any bootable image in the Flash, download the IOS Image File by using X-Modem. 2. Enter the **set BOOT flash:** *name of IOS file* command to set the boot variable to the file name displayed in Step 1. **Note** BOOT must be capitalized and make sure to include flash: before the file name. 3. Enter the **boot** command. **Note** If the switch boots properly, enter the **setting boot parameters** global configuration command to verify and set the BOOT parameters (if needed), and proceed to Step 4. If the switch fails to boot properly, download the IOS Image File using X-Modem. 4. After setting the BOOT parameters, reload the switch by entering the **reload** privileged EXEC command. The switch boots up automatically with the correct image.

Table 9-4 Problems Encountered When Upgrading the Switch (continued)

Problem	Suggested Solution
Failed software upgrade; switch is resetting continuously.	This might be due to a corrupt or incorrect image, or the image in Flash might be missing. Following these steps to recover if the switch is in a reset loop after or during the upgrade. 1. Connect the PC to the switch console port. 2. Press the **Enter** key a few times. Are you seeing a `switch: prompt`? If not, go to Step 3. Otherwise, go to Step 4. 3. Disconnect the power cord. Hold down the mode button on the front of the switch, and plug the power cord back in. All LEDs above all ports should come on green. Continue to hold down the mode button until the light above port 1 goes out, and then release the mode button. The prompt should be *switch:*. 4. Download the IOS Image File using X-Modem.
After the upgrade, the switch still boots up with the old image.	This happens when either the BOOT parameters are not correct and the switch is still set to boot from the old image or the upgrade did not go through properly. Verify the BOOT parameters, and correct them if needed. • If the BOOT parameters are correct, download the IOS Image File using TFTP. • If the switch still boots with the old image, download the IOS Image File using X-Modem.
Switch not booting automatically; needs a manual boot at the ROMMON (`switch: prompt`).	The switch boot parameters might be set for manual boot. The switch can be set to boot automatically by following these steps: 1. Use Telnet to access the switch, or connect the PC to the switch console port. 2. Enter the privileged EXEC mode by entering the **enable** command at the `switch> prompt`. 3. Enter the global configuration mode by entering **configure terminal** at the `Switch# prompt`. 4. Enter **no boot manual** to tell the switch to boot automatically. 5. Enter **end** to return to privileged EXEC mode, and save the configuration by entering the **write memory** command. 6. Verify the boot parameters by entering **show boot**. Verify that Manual Boot is set to *no*.

Recovery Procedures

The recovery procedures in this section require that you have physical access to the switch. Recovery procedures include the following topics:

- 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 the following port-configuration conflicts:

- Member switches cannot connect to the command switch through a port that is defined as a network port. For information on the network port feature, see the "Enabling a Network Port" section on page 7-7.
- 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 5-11.
- Member switches connected to the command switch through a secured port can lose connectivity if the port is disabled due to a security violation. Secured ports are described in the "Enabling Port Security" section on page 7-15.

Recovering from a Command Switch Failure

This section describes how to recover from a failed command switch. If you are running IOS Release 12.0(5)XU, you can configure a redundant command switch group by using the Hot Standby Router Protocol (HSRP). For more information, see the "Designating and Enabling Standby Command Switches" section on page 5-17.

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 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 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
- Replacing a failed command switch with another switch

For a list of command-capable Catalyst desktop switches, see the release notes.

Replacing a Failed Command Switch with a Cluster Member

Follow these steps to replace a failed command switch with a command-capable member of the same cluster:

Step 1 Disconnect the command switch from the member switches, and physically remove it from the cluster.

Step 2 Use a member switch in place of the failed command switch, and duplicate its connections to the cluster members.

Step 3 Start a command-line interface (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 installation guide.

Step 4 At the switch prompt, change to privileged EXEC mode:

```
Switch> enable
Switch#
```

Step 5 Enter the password of the *failed command switch*.

Step 6 From privileged EXEC mode, enter global configuration mode.

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Step 7 From global configuration mode, remove previous command-switch information from the switch.

```
Switch(config)# no cluster commander-address
```

Step 8 Return to privileged EXEC mode.

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

Step 9 Use the setup program to configure the switch IP information.

This program prompts you for an IP address, subnet mask, default gateway, and password. From privileged EXEC mode, enter **setup**, and press **Return**.

```
Switch# setup
         --- System Configuration Dialog ---
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 '[]'.
Continue with configuration dialog? [yes/no]:
```

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

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

Step 11 Enter the switch IP address, and press **Return**:

```
Enter IP address: ip_address
```

Step 12 Enter the subnet mask, and press **Return**:

```
Enter IP netmask: ip_netmask
```

Step 13 Enter **Y** at the next prompt to specify a default gateway (router):

```
Would you like to enter a default gateway address? [yes]: y
```

Step 14 Enter the IP address of the default gateway, and press **Return**.

```
IP address of the default gateway: ip_address
```

Step 15 Enter a host name for the switch, and press **Return**.

Note 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 character in a host name for any switch.

```
Enter a host name: host_name
```

Step 16 Enter the password of the *failed command switch*, and press **Return**.

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

```
Enter enable secret: secret_password
```

Step 17 Enter **Y** to enter a Telnet password:

```
Would you like to configure a Telnet password? [yes] y
```

Note The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

Step 18 Enter the Telnet password, and press **Return**:

```
Enter Telnet password: telnet_password
```

Step 19 Enter **Y** to configure the switch as the cluster command switch. Enter **N** to configure it as a member switch or as a standalone switch.

Note If you enter **N**, the switch appears as a candidate switch in Cluster Builder. In this case, the message in Step 20 is not displayed.

```
Would you like to enable as a cluster command switch? y
```

Step 20 Assign a name to the cluster, and press **Return**.

```
Enter cluster name: cls_name
```

Note The cluster name can be 1 to 31 alphanumeric characters, dashes, or underscores.

Step 21 The initial configuration is displayed:

```
The following configuration command script was created:

ip subnet-zero
interface VLAN1
ip address 172.20.153.36 255.255.255.0
ip default-gateway 172.20.153.01
hostname host_name
enable secret 5 $1$M3pS$cXtAlkyR3/6Cn8/
line vty 0 15
password telnet_password
snmp community private rw
snmp community public ro
cluster enable cls_name

end
```

Step 22 Verify that the information is correct.

- If the information is correct, enter **Y** at the prompt, and press **Return**.
- If the information is not correct, enter **N** at the prompt, press **Return**, and begin again at Step 1.

```
Use this configuration? [yes/no]: y
```

Step 23 Start your browser, and enter the switch IP address that you entered in Step 11.

Step 24 Display the VSM Home page for the switch, and select **Enabled** from the Command Switch drop-down list.

Step 25 Click **Cluster Management**, and display Cluster Builder.

CMS prompts you to add candidate switches. The password of the failed command switch is still valid for the cluster, and you should enter it when candidate switches are proposed for cluster membership.

Replacing a Failed Command Switch with Another Switch

Follow these steps when you are replacing a failed command switch with a switch that is command-capable but not part of the cluster:

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, change to 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 an IP address, subnet mask, default gateway, and password. From privileged EXEC mode, enter **setup**, and press **Return**.

```
Switch# setup
         --- System Configuration Dialog ---
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 '[]'.
Continue with configuration dialog? [yes/no]:
```

Step 6 Enter **Y** at the first prompt.

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

Step 7 Enter the switch IP address, and press **Return**:

```
Enter IP address: ip_address
```

Step 8 Enter the subnet mask, and press **Return**:

```
Enter IP netmask: ip_netmask
```

Step 9 Enter **Y** at the next prompt to specify a default gateway (router):

```
Would you like to enter a default gateway address? [yes]: y
```

Step 10 Enter the IP address of the default gateway, and press **Return**.

```
IP address of the default gateway: ip_address
```

Step 11 Enter a host name for the switch, and press **Return**.

Note 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 character in a host name for any switch.

```
Enter a host name: host_name
```

Step 12 Enter the password of the *failed command switch*, and press **Return**.

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

```
Enter enable secret: secret_password
```

Step 13 Enter **Y** to enter a Telnet password:

```
Would you like to configure a Telnet password? [yes] y
```

Note The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

Step 14 Enter the Telnet password, and press **Return**:

```
Enter Telnet password: telnet_password
```

Step 15 Enter **Y** to configure the switch as the cluster command switch. Enter **N** to configure it as a member switch or as a standalone switch.

Note If you enter **N**, the switch appears as a candidate switch in Cluster Builder. In this case, the message in Step 20 is not displayed.

```
Would you like to enable as a cluster command switch? y
```

Step 16 Assign a name to the cluster, and press **Return**.

```
Enter cluster name: cls_name
```

Note The cluster name can be 1 to 31 alphanumeric characters, dashes, or underscores.

Step 17 The initial configuration is displayed:

```
The following configuration command script was created:

ip subnet-zero
interface VLAN1
ip address 172.20.153.36 255.255.255.0
ip default-gateway 172.20.153.01
hostname host_name
enable secret 5 $1$M3pS$cXtAlkyR3/6Cn8/
line vty 0 15
password telnet_password
snmp community private rw
snmp community public ro
cluster enable cls_name

end
```

Step 18 Verify that the information is correct.

- If the information is correct, enter **Y** at the prompt, and press **Return**.
- If the information is not correct, enter **N** at the prompt, press **Return**, and begin again at Step 1.

```
Use this configuration? [yes/no]: y
```

Step 19 Start your browser, and enter the switch IP address that you entered in Step 7.

Step 20 Click **Cluster Manager Suite or Visual Switch Manager**, and display Cluster Builder.

It prompts you to add the candidate switches. The password of the failed command switch is still valid for the cluster. Enter it when candidate switches are proposed for cluster membership, and click **OK**.

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 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 9-14.

Recovering from a Lost or Forgotten Password

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 console port. For more information, refer to the switch installation guide.

Note You can configure your switch for Telnet by following the procedure in the "Accessing the CLI" section on page 3-8.

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. The following 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:

```
switch: dir flash:
```

The switch file system is displayed:

```
Directory of flash:

  2  -rwx      843947   Mar 01 1993 00:02:18 C2900XL-h-mz-112.8-SA
  4  drwx        3776   Mar 01 1993 01:23:24  html
 66  -rwx         130   Jan 01 1970 00:01:19  env_vars
 68  -rwx        1296   Mar 01 1993 06:55:51  config.text

1728000 bytes total (456704 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 following 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.

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 Unplug 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.