



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 Cluster Manager Suite (CMS) to identify and solve problems.

This chapter describes how to perform the following tasks:

- Identify an autonegotiation mismatch
- Recover from corrupted software
- Recover from a lost or forgotten password
- Recover from a failed command switch
- Maintain connectivity with cluster members

Autonegotiation Mismatches

The IEEE 802.3u autonegotiation protocol manages the switch settings for speed (10 Mbps or 100 Mbps) 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 in 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.

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

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 into Flash memory.
- 

## 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 “Configuring the Switch for Telnet” section on page 2-39.

---

- Step 2** Set the line speed on the emulation software to 9600 baud.
- Step 3** Unplug the switch power cord.
- Step 4** Press in 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 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 “Building a Redundant Cluster” section on page 3-17.

**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 information on command-capable switches, see the “Supported Hardware” section on page 1-3.

### 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** 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 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 the member switch from the cluster.
- ```
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
```
- If this prompt does not appear, enter **enable**, and press **Return**. Enter **setup**, and press **Return** to start the setup program.
- Step 11** Enter the switch IP address, and press **Return**:
- ```
Enter IP address: ip_address
```
- Step 12** Enter the subnet mask (IP netmask) address, and press **Return**:
- ```
Enter IP netmask: ip_netmask
```

**Step 13** Enter **Y** to enter a default gateway (router) address:

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

**Step 14** Enter the IP address of the default gateway (router), and press **Return**:

Enter router IP address: *IP\_address*

**Step 15** Enter a host name, and press **Return**:

Enter host name: *host\_name*

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

Enter enable secret password: *secret\_password*

**Step 17** Enter a Telnet password, and press **Return**:

Would you like to configure a telnet password? [yes]: **y**

Enter telnet password: *password*

The initial configuration displays:

The following configuration command script was created:

```
ip subnet-zero
interface VLAN1
ip address IP_address IP_netmask
ip default-gateway IP_address
hostname host_name
enable secret 5 1yDsa$/YLihJcV8e/HODagkW1Ff0
line vty 0 15
password password
snmp community private rw
snmp community public ro
!
end
```

Use this configuration? [yes/no]:

**Step 18** Verify that the addresses are correct.

**Step 19** Enter **Y**, and press **Return** if the displayed information is correct.

If this information is not correct, enter **N**, press **Return**, and begin again at Step 9.

**Step 20** Start your browser, and enter the IP address you just entered for the switch.

**Step 21** Display the VSM Home page for the switch, and select **Enabled** from the Command Switch drop-down list.

**Step 22** 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.



---

**Note** You can also add switches to the cluster by using the CLI. For the complete instructions, see the “Adding and Removing Member Switches” section on page 3-12.

---

## 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 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**

If this prompt does not appear, enter **enable**, and press **Return**. Enter **setup**, and press **Return** to start the setup program.

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

Enter IP address: *ip\_address*

**Step 8** Enter the subnet mask (IP netmask) address, and press **Return**:

Enter IP netmask: *ip\_netmask*

**Step 9** Enter **Y** to enter a default gateway (router) address:

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

**Step 10** Enter the IP address of the default gateway (router), and press **Return**:

Enter router IP address: *IP\_address*

**Step 11** Enter a host name, and press **Return**:

Enter host name: *host\_name*

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

Enter enable secret password: *secret\_password*

**Step 13** Enter a Telnet password, and press **Return**:

Would you like to configure a telnet password? [yes]: **y**

Enter telnet password: *password*

The initial configuration displays:

The following configuration command script was created:

```
ip subnet-zero
interface VLAN1
ip address IP_address IP_netmask
ip default-gateway IP_address
hostname host_name
enable secret 5 1yDsa$/YLihJcV8e/HODagkW1Ff0
line vty 0 15
password password
snmp community private rw
snmp community public ro
!
end
```

Use this configuration? [yes/no]:

- Step 14** Verify that the addresses are correct.
- Step 15** Enter **Y**, and press **Return** if the displayed information is correct.  
If this information is not correct, enter **N**, press **Return**, and begin again at Step 5.
- Step 16** Start your browser, and enter the IP address you just entered for the switch.
- Step 17** 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**.



---

**Note** You can also add switches to the cluster by using the CLI. For the complete instructions, see the “Adding and Removing Member Switches” section on page 3-12.

---

## 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 4-23.
- Member switches must connect to the command switch through a port that belongs to the same management VLAN. For more information, see the “Understanding Management VLAN Changes” section on page 3-4.
- 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 4-51.

