Using the Management Interfaces

This chapter describes the features and characteristics of the management interfaces. You can use a web browser such as Netscape Communicator or Microsoft Internet Explorer to access these interfaces to monitor and configure a switch or a group of switches.

This chapter describes how to perform the following tasks:

- Prepare to use the web-based management interfaces

- Use the Cisco Visual Switch Manager (CVSM) interface for managing a switch

  With CVSM, you can configure and monitor a switch by using a graphical user interface. Individual switch configuration information is provided in Chapter 3, "Managing Your Switches."

- Use the Switch Network View interface for managing a simple stack of switches

  With Switch Network View, you can manage a stack of up to five switches configured in a star topology. Each switch has its own IP address. You can display a map of the stack and information about the devices and links that connect them. Stack configuration information is provided in Chapter 3, "Managing Your Switches."

- Use the Cluster Management interface for managing a cluster of switches

  With Cluster Management, you can use a command switch with an IP address to manage a cluster of up to 15 other switches. The other switches, called *member* switches, do not need individual IP addresses. Cluster configuration information is provided in Chapter 4, "Managing Clusters of Switches."

- Use the IOS command-line interface (CLI) to manage a switch or group of switches.

  The CLI is accessed through the console port or Telnet. Individual switch configuration procedures are provided in Chapter 3, "Managing Your Switches" and Chapter 4, "Managing Clusters of Switches."

- Use SNMP MIB objects to manage a switch or group of switches.

    The MIBs are accessed through an SNMP management application.

    Table 3-1 on page 3-2 lists the key features and defaults of this release and cross-references the descriptions for changing them with the CLI or an HTML interface.

Preparing to Use the Web-Based Management Interfaces

All of the web-based management features are based on an embedded HTML web server in the switch Flash memory. This section describes how to configure your environment for web-based management.

Note   Web-based management uses HTTP, an in-band form of communication: you access the switch through one of its Ethernet ports. Therefore, be sure that you do not disable or otherwise misconfigure the port through which *you* are communicating with the switch. When you install the switch, you might want to write down the port number that you are using. In addition, you must have privilege level 15 to access the web-based management applications (CVSM, Switch Network View, and Cluster Management). For more information, see the "Setting Passwords and Privilege Levels" section on page 2-32.

Hardware and Software Requirements

You can access the web-based interfaces through the browsers listed in Table 2-1. The switch checks the browser version when starting a session to ensure that the browser is supported. If the browser is not supported, the switch displays an error message, and the session does not start.

The minimum requirement for a PC is a Pentium processor running at 166 MHz with 64 MB of DRAM. The minimum requirement for a UNIX workstation is a Sun Ultra 1 running at 143 MHz.

Note   In Cluster Management, Internet Explorer versions 4.01 and 5.0 display only edge devices connected to the command switch. Other functionality is similar to that of Netscape Communicator.

The following operating systems are supported for web-based management:

- Microsoft Windows 95 (Service Pack 1 required)

- Microsoft Windows 98, second edition

- Microsoft Windows NT 4.0 (Service Pack 3 required)

- Solaris 2.5.1 or higher, with the Sun-recommended patch cluster for that operating system and Motif library patch 103461-24

Table 2-1   Browser Support for Web-based Management

Browser	Minimum Version	Supported Versions
Netscape Communicator	4.5	4.5, 4.51, 4.61[1]
Internet Explorer[2]	4.01a	4.01a, 5.0

1   Netscape Communicator 4.6 is not supported.
2   Not supported on Solaris 2.5.1 or higher.

Table 2-2 lists the configuration that yields the best results for web-based management.

Table 2-2   Recommended Platform Configuration for Web-based Management

OS	Processor Speed	DRAM	Number of Colors	Resolution	Font Size
Windows NT 4.0	Pentium 300 MHz	128 MB	65536	1024 x 768	Small
SunOS 5.6	Sparc 333 MHz	128 MB	Most colors for applications	—	Small (3)

Configuring Netscape Communicator

Follow these steps to configure Netscape Communicator:

Step 1   Start Netscape Communicator.

Step 2   From the menu bar, select **Edit>Preferences**.

Step 3   In the Preferences window, click **Advanced**.

(a)   Select the **Enable Java**, **Enable JavaScript**, and **Enable Style Sheets** check boxes.

(b)   Click **OK** to return to the browser Home page.

Step 4   From the menu bar, select **Edit>Preferences**.

(a)   In the Preferences window, click **Advanced Cache**, and select **Every time**.

(b)   Click **OK** to return to the browser Home page.

Configuring Microsoft Internet Explorer 4.01

Follow these steps to configure Microsoft Internet Explorer 4.01:

Step 1   Start Internet Explorer.

Step 2   From the menu bar, select **View>Internet Options**.

Step 3   In the Internet Options window, click the **Advanced** tab.

(a)   Scroll through the list of options until you see Java VM. Select the **Java logging enabled** and **Java JIT compiler enabled** check boxes.

(b)   Click **Apply**.

Step 4   In the Internet Options window, click the **General** tab.

(a)   In the Temporary Internet Files section, click the **Settings...** button.

(b)   In the Settings window, select **Every visit to the page**, and click **OK**.

Step 5   In the Internet Options window, click the **Security** tab.

(a)   In the Zone drop-down list, select **Trusted Sites Zone**.

(b)   In the Trusted Sites Zone section, select **Custom**.

(c) Click the **Settings...** button.

Step 6 In the Security Settings window, scroll to the **Java>Java Permissions** section, and select **Custom**.

Click the **Java Custom Settings...** button, which appears at the bottom of the window.

Step 7 In the Trusted Sites Zone window, click the **Edit Permissions** tab.

(a) If the buttons under **Run Unsigned Content** are not available, select either **Medium** or **Low** security in the Reset Java Permissions list box. Click **Reset**.

(b) Under **Run Unsigned Content**, select **Enable**, and click **OK**.

Step 8 In the Security Settings window, click **OK**.

Step 9 In the Internet Options window, click the **Security** tab.

(a) Verify that the Zone drop-down list is set to **Trusted Sites Zone**.

(b) In the Trusted Sites Zone section, click the **Add Sites...** button.

Step 10 In the Trusted Sites Zone window, deselect the **Require server verification** check box.

(a) In the **Add this Web site to the Zone** field, enter the IP address of the switch you want to manage, as in this example:

```
http://172.20.153.36
```

Note If you plan to use Cluster Management for switch configuration, you must enter the IP address of the command switch. You can enter the addresses of member switches, but they are not required.

If you plan to use CVSM for switch configuration, you must enter the IP address of each switch that you want to manage. You do not need to delete the address from the trusted site list if the switch later becomes a cluster member.

(b) Click **Add**, and then click **OK**.

Step 11 In the Internet Options window, click **OK**.

Configuring Microsoft Internet Explorer 5.0

Note During the installation of this browser, make sure to select the **Install Minimal or Customize Your Browser** check box. Then in the Component Options window, in the Internet Explorer 5 section, make sure to select the **Microsoft Virtual Machine** check box, which allows you to display applets written in Java.

Follow these steps to configure Microsoft Internet Explorer 5.0:

Step 1 Start Internet Explorer.

Step 2 From the menu bar, select **Tools>Internet Options**.

Step 3 In the Internet Options window, click the **Advanced** tab.

    (a) Scroll through the list of options until you see Java VM. Select the **Java logging enabled** and **JIT compiler for virtual machine enabled** check boxes.

    (b) Click **Apply**.

Step 4 In the Internet Options window, click the **General** tab.

    (a) In the Temporary Internet Files section, click the **Settings...** button.

    (b) In the Settings window, select **Every visit to the page**, and click **OK**.

Step 5 In the Internet Options window, click the **Security** tab.

    (a) Select the **Trusted Sites** icon and click the **Sites...** button.

    (b) Deselect the **Require server verification** check box.

    (c) Add the switches you want to manage by entering their URLs in the **Add this web site to the zone** field. Click the **Add** button to add each switch.

A URL is the switch IP address preceded by **http://**. For example, you might enter:

```
http://172.20.153.36
```

> **Note** If you plan to use Cluster Management for switch configuration, you must enter the IP address of the command switch. You can enter the addresses of member switches, but they are not required.
>
> If you plan to use CVSM for switch configuration, you must enter the IP address of each switch that you want to manage. You do not need to delete the address from the trusted site list if the switch later becomes a cluster member.

    (d)   After you have finished entering the URLs for your switches, click **OK**.

Step 6   While still in the Security tab of Internet Options window, click the **Custom Level...** button.

    (a)   In the **Security Settings** window, scroll to the **Java>Java permissions** section.

        If you do not see this section, you need to reinstall the browser, and follow the instructions in the note at the beginning of this procedure.

    (b)   Select **Custom** to enable the **Java Custom Settings** button.

    (c)   Click the **Java Custom Settings...** button.

Step 7   In the Trusted Sites window, click the **Edit Permissions** tab.

    (a)   Under Run Unsigned Content, select **Enable**.

    (b)   Click **OK**.

Step 8   In the Security Settings window, click **OK**.

Step 9   In the Internet Options window, click **OK**.

> **Note** If you are using Microsoft Internet Explorer 5.0 to make configuration changes to the switch, be aware that this browser does not reflect the latest configuration changes. Make sure you click the browser **Refresh** button for every configuration change.

Using Cisco Visual Switch Manager

CVSM is a web-based device-management application for configuring and monitoring your switch. Because the switch is preconfigured, CVSM shows the settings that the switch is using. You change the configuration settings by entering information in fields, adding and removing list items, or selecting check boxes. In addition, the CVSM Home page displays an image of the switch (Figure 2-2). The LEDs reflect the current status of the switch, and you can click on ports to configure them.

When you enter information in a CVSM field and click **Apply**, the change becomes part of the running (current) configuration. If you make a mistake and want to retype an entry, click **Cancel** to undo your first entry. Items added to or removed from lists in CVSM *immediately* become part of the running configuration, and you do not need to click **Apply**.

Note   The current configuration is not necessarily the startup configuration. Save the configuration as the startup configuration in CVSM by following the procedure in "Saving the Configuration File" section on page 3-39. You can also save the configuration with the CLI; see the "Working with Files in Flash Memory" section on page 2-37.

## Accessing CVSM for the First Time

The switch must have an IP address before you can use CVSM to manage the switch. By contrast, a cluster requires only one IP address per cluster. For instructions on assigning the IP address, see the "CLI Procedure for Assigning IP Information to the Switch" section on page 3-52. For information on clustering, see the "Using Cluster Management" section on page 2-16 and Chapter 4, "Managing Clusters of Switches."

Follow these steps to access CVSM:

Step 1 Be sure that you have configured your browser correctly.

For more information, see the "Preparing to Use the Web-Based Management Interfaces" section on page 2-2.

Step 2 Start the browser.

Step 3 Enter the switch IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer).

Step 4 Press **Return**.

Step 5 Enter your username and password when prompted.

The password provides level 15 access.

The Cisco Systems Access page (Figure 2-1) is displayed.

Step 6 Click **Visual Switch Manager** to display the CVSM Home page (Figure 3-4).

Figure 2-1   Cisco Systems Access Page
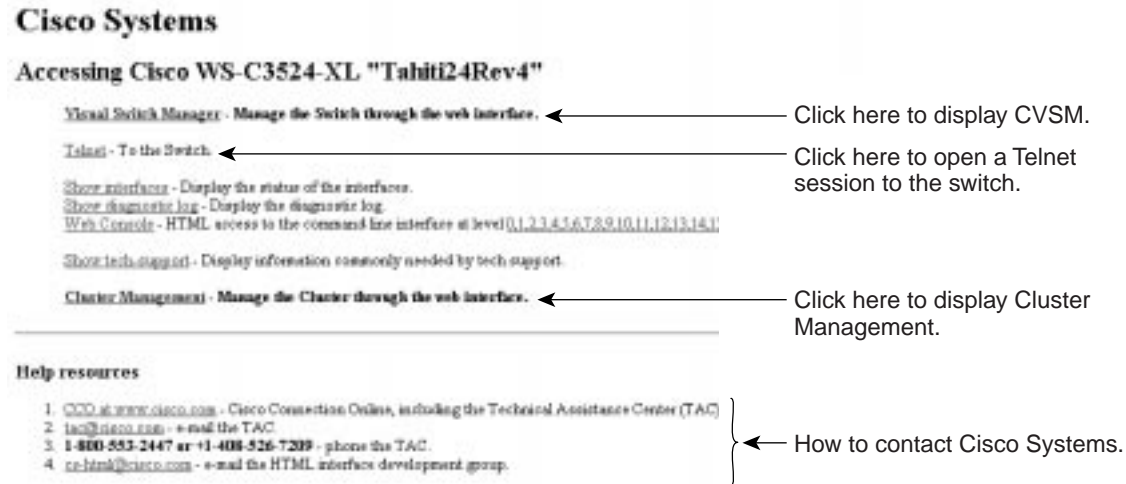
All the CVSM pages have a Home button that you can click to return to this page. From the Home page, you can monitor and configure the port as shown in Figure 2-2.

The other web-based applications, Cluster Management and Switch Network View, are available from the CVSM Home page:

- If your switch is part of a cluster, you can click **Cluster Management** to create and manage clusters of switches. To use the switch cluster capabilities, you must enable one switch as the command switch and name the cluster on the CVSM home page.

- If your switch is not part of a cluster, you can click **Switch Network View** to display the stack connected to the switch.
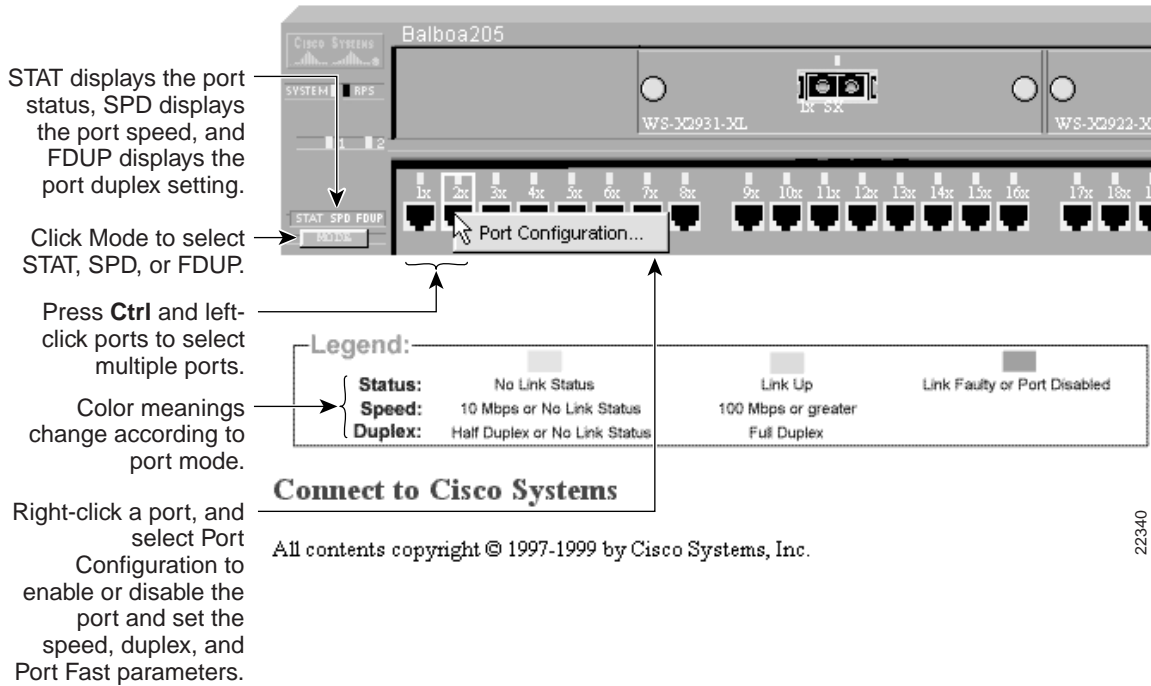
You can bookmark the IP address to easily retrieve the Home page for later use.

Note   If you are working with clusters of switches, limit your bookmarks to command-switch pages.

Figure 2-2   Using the Mode Button to Configure Ports

STAT displays the port status, SPD displays the port speed, and FDUP displays the port duplex setting.

Click Mode to select STAT, SPD, or FDUP.

Press **Ctrl** and left-click ports to select multiple ports.

Color meanings change according to port mode.

Right-click a port, and select Port Configuration to enable or disable the port and set the speed, duplex, and Port Fast parameters.

CVSM Menu Options

You can access the device-management features from the Home page menu bar drop-down menus, such as the Port menu shown in Figure 2-3. Table 2-3 describes the menu options and their function.

Figure 2-3 **CVSM Menu Bar**

| Port | System | Security | Device | VLAN | Fault |

Port Configuration
Port Grouping (EC)
Switch Port Analyzer (SPAN)
Flooding Controls

14035

Table 2-3 **Cisco Visual Switch Manager Menu Options**

Menu Bar Choices	Task
Port	
Port Configuration	Enable or disable ports and set port parameters.
Port Grouping (EC)	Group ports into logical units for high-speed links between switches.
Switch Port Analyzer (SPAN)	Enable SPAN port monitoring.
Flooding Controls	Enable broadcast storm control, assign a network port, and block unicast and multicast flooding on a per-port basis.
System	
System Configuration	Save the running configuration, and upgrade firmware through the Trivial File Transfer Protocol (TFTP).
System Time Management	Configure the time on the switch or configure the switch to receive the time from a Network Time Protocol (NTP) server.
IP Management	Enter IP information for the switch. Configure the management VLAN interface.
SNMP Configuration	Enter SNMP trap managers and community strings.
ARP Table	Display the ARP table and change the timeout setting.
Security	
Address Management	Enter static and secure addresses; change the dynamic address aging time.
Port Security	Enable port security.

Table 2-3   Cisco Visual Switch Manager Menu Options (continued)

Menu Bar Choices	Task
Device	
Cisco Discovery Protocol	Enable and disable CDP information.
Cisco Group Management Protocol	Enable and disable CGMP and CGMP Fast Leave feature.
Spanning-Tree Protocol	Display and change STP parameters for the switch.
VLAN	
VLAN Membership	Assign ports to port-based VLANs.
Fault	
Logging Config	Set logging parameters.

Using Switch Network View

The Switch Network View page displays a map of the devices that are directly connected to a switch that is not part of a cluster. From this page, you can display switch connection information, device reports, and link reports.

You display Switch Network View from the CVSM home page, but its availability depends on how your switch is configured. If your switch is part of a cluster, the **Cluster Management** button displays. If your switch is not part of a cluster, the **Switch Network View** button displays.

If your switch is not in a cluster, click **Switch Network View** to display the view shown in Figure 2-4. Blue labels identify stack members, which include 2900 and 3500 XL switches. Yellow labels identify generic edge devices connected to stack members. Edge devices include Cisco routers, switches, hubs, and Cisco Micro Webservers if they are directly attached to a 2900 or 3500 XL switch. For information on the supported IOS Release for these switches, see Table 1-1 on page 1-4.

Using Switch Network View Buttons

Table 2-4 describes the Switch Network View buttons and how to use them.

Table 2-4   **Switch Network View Buttons**

Name	Purpose
Visual Stack	Displays images of stack members. From this page you can: • Display the status, duplex, speed and Port Fast settings on this port. • Configure ports. • Start the CVSM for any stack member.
Switch Manager	Displays switch connection information (device type, IP address, port number) for switches that are directly connected to the primary switch. Switch stack members have blue labels, and switch edge devices have yellow labels. Click the IP address of a stack member to display the CVSM Home page for the switch.
Toggle Labels	Alternates between displaying IP addresses and device type labels.
Help	Displays online help.
Legend	Displays the meanings of icons and links.

Figure 2-4   Switch Network View Page
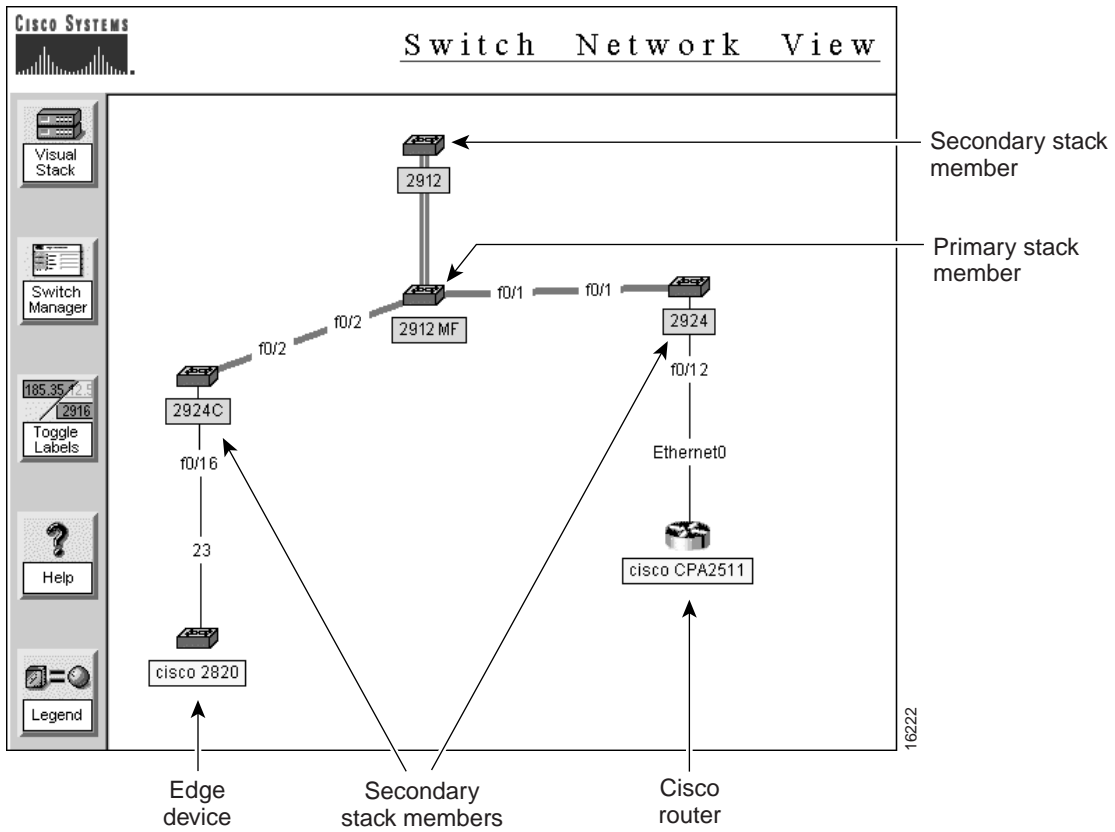
Accessing Device Menus

To display the device pop-up menu, right-click a switch. You can select one of the following options:

- Device Report—Displays the device report for the switch. The device report has three pages of switch information: configuration, system, and port.

- Switch Manager—Displays the CVSM Home page for the switch.

Accessing Link Menus

To display the link report, right-click a link, and select **Link Report**. This report displays the link speed, VLAN and port group memberships, and the STP state.

Using Cluster Management

Cluster Management consists of three related applications that you can use to create clusters of switches, manage individual switches, and display device information, link information, and performance graphs. Each cluster requires a designated command switch with an IP address to manage and communicate all cluster-wide management functions.

This section describes how you can use the following Cluster Management applications to manage your network:

- Cluster Builder

- Cluster View

- Cluster Manager

To use the switch cluster capabilities, you must enable one switch as the command switch and name the cluster on the CVSM home page. You can also perform these tasks with the CLI.

Accessing Cluster Management

Once the cluster is created, you can access Cluster Management in the following ways:

- Click **Cluster Management** on the Cisco Systems Access page (Figure 2-1).

  This link is present if the switch is running command-capable clustering software with the command switch functionality enabled (functioning as the command switch).

- Click **Cluster Management** on the CVSM Home page (Figure 3-4).

  This button appears if the switch is command capable and enabled (functioning as the command switch), if the switch is command capable and disabled, or if the switch is a member of a cluster.

For information on how to create a cluster, see the "Creating Clusters" section on page 4-5.

Common Interface Features in Cluster Management

Certain features are common to all three Cluster Management applications. Table 2-5 lists the buttons on the Cluster Builder, Cluster View, and Cluster Manager pages.

Table 2-5 **Cluster Management Buttons**

Button	Action
Legend	Provides a legend with the meaning of icons, labels, and links.
Save Config	Saves the current configuration to permanent storage on the 2900 and 3500 XL command and member switches. These configurations are saved in the config.text file that is used when the switches are reset. Click this button for all configuration changes except for saving the device layout or when making changes in the User Settings window. For more information, see the "Working with Files in Flash Memory" section on page 2-37.
	This button does not apply to Catalyst 1900 and 2820 switches, which automatically save configuration changes to Flash memory as they occur.

Table 2-5   Cluster Management Buttons (continued)

Button	Action
User Settings	Configures your preferences for Cluster Management. The command switch saves this information in permanent storage, and you do not need to click **Save Config**. You can set these preferences to: • Display suggested candidates every time Cluster Builder starts • Display Cluster Builder or Cluster Manager page by default • Polling interval for performance graphs • Polling interval for Cluster Builder and Cluster Manager For more information, see the "Changing User Settings" section on page 4-17.
Help	Displays detailed procedures for cluster management tasks.

Using Cluster Builder

Use Cluster Builder to automatically or manually create a cluster of switches. Switches directly connected to the command switch that are running the appropriate software display themselves as cluster members or candidates.

Depending on your topology, you can add all candidate switches to the cluster at once (star topology) or add them one by one (daisy-chain topology). Figure 2-5 shows Cluster Builder displaying a map of cluster devices.
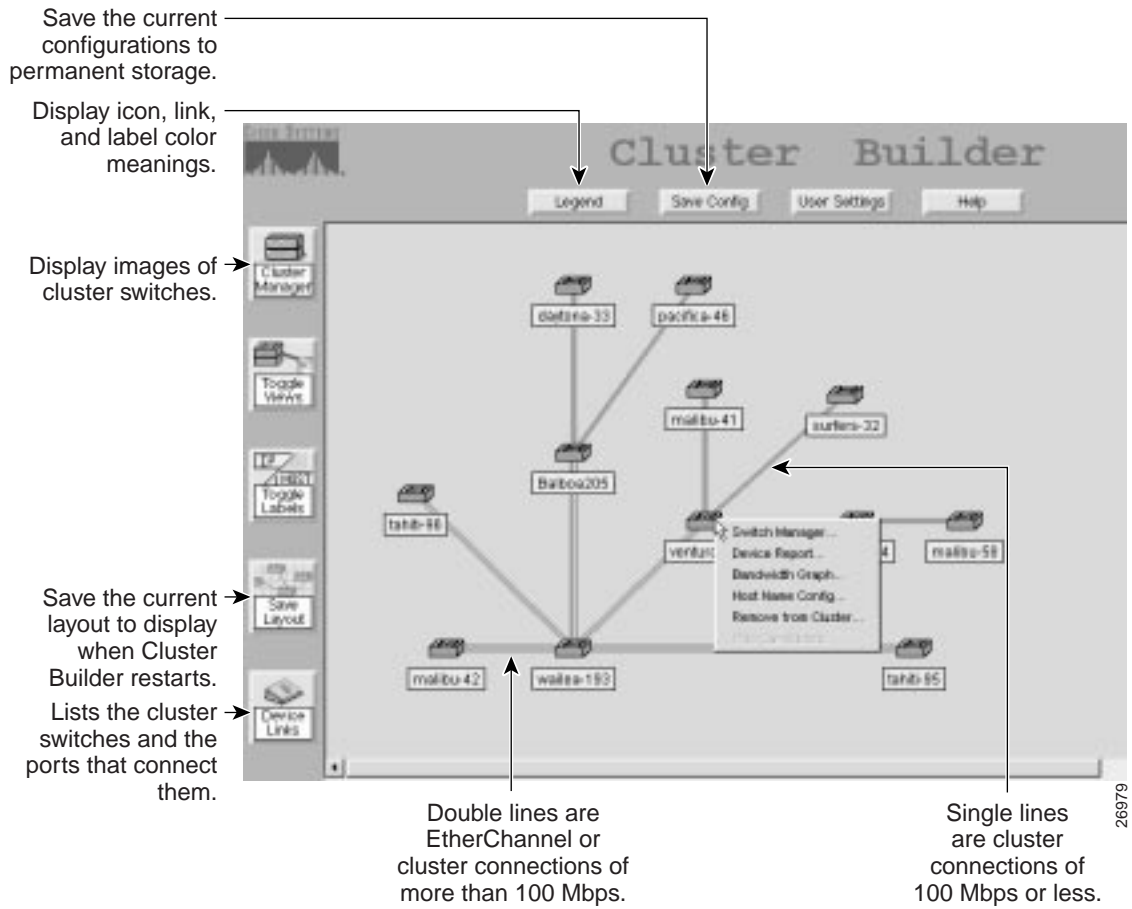
Cluster Builder labels other network devices with the following colors:

Green   A cluster member, either as a member switch or as the command switch.

Blue   A cluster candidate that is fully qualified to become a cluster member. Add these candidates to the cluster with Cluster Builder.

Table 2-6 describes the active buttons in Cluster Builder, Table 2-7 describes the available menu options when you right-click a switch, and Table 2-8 describes the available menu options when you right-click a link. The menu options can vary depending on the type of device and whether or not it is a cluster member.

Figure 2-5   Cluster Builder

Save the current configurations to permanent storage.

Display icon, link, and label color meanings.

Display images of cluster switches.

Save the current layout to display when Cluster Builder restarts.

Lists the cluster switches and the ports that connect them.

Double lines are EtherChannel or cluster connections of more than 100 Mbps.

Single lines are cluster connections of 100 Mbps or less.

Table 2-6 **Cluster Builder Buttons**

Button	Action
Cluster Manager	Displays Cluster Manager.
Toggle Views	Toggles between Cluster View and Cluster Builder. In Cluster View, all cluster switches are represented by a double-switch icon. Candidate switches and edge devices are also displayed.
Toggle Labels	Changes the labels on the links and icons. The labels can be • MAC address (IP address of the command switch) of the switch and the port numbers that connect links. A candidate switch also displays its IP addresses if one is assigned. • Host name.
Save Layout	Saves the current layout of the switch icons. As long as there are no topology changes, the saved layout displays the next time you display Cluster Builder. For more information, see the "Arranging and Saving the Device Layout" section on page 4-16.
Device Links	Displays port connection information for cluster members. For more information, see the "Displaying Port Connection Information" section on page 4-25.

(continued)

Table 2-7 **Cluster Builder Device Menu Items**

Menu Item	Action (available when you right-click a switch)
Switch Manager	Displays the switch manager home page. You can also display this page by double-clicking the command, member, or candidate switches. For more information, see the "Managing Your Switch through CVSM" section on page 3-14.
Device Web Page	Displays the HTML interface for the device. (Not always displayed.)
Device Report	Displays the device report for the switch. The device report has three pages of information about the switch: configuration, system, and port. This feature is not available on Catalyst 1900 and 2820 switches. For more information, see the "Displaying Device Reports and Graphs" section on page 4-42.

Table 2-7   Cluster Builder Device Menu Items (continued)

Menu Item	Action (available when you right-click a switch)
Bandwidth Graph	Displays a graph that plots the total bandwidth used by the switch. This feature is not available on Catalyst 1900 and 2820 switches. For more information, see the "Displaying Device Reports and Graphs" section on page 4-42.
Host Name Config	Displays a window where you can enter a host name for the switch. For more information, see the "Changing the Host Name" section on page 4-25.
Add to Cluster, Remove from Cluster	Adds or removes the selected switch to or from the cluster. (Not always displayed.) For more information, see the "Adding and Removing Member Switches" section on page 4-12.
Hide Candidates, Show Candidates	Hides or redisplays candidate switches connected to a cluster member.

Table 2-8   Cluster Builder Link Menu Items

Menu Item	Action (available when you right-click a link)
Link Graph	Displays the performance graph for the link. You can plot the link utilization percentage and the total packets, bytes, and errors recorded on the link. To display a link graph, one end of the link must be connected to a port on a cluster member that is a 2900 or 3500 XL switch. Links between Catalyst 1900 and 2820 switches, Catalyst 2820 and 2820 switches, or Catalyst 1900 and 1900 switches cannot be graphed. For more information, see the "Displaying Link Utilization Graphs" section on page 4-37.

Using Cluster View

Cluster View displays the cluster as a double-switch icon with connections to edge devices and candidate switches. To access Cluster View, click the **Toggle Views** button in Cluster Builder.

Figure 2-6   Cluster View

Cluster View labels network devices with the following colors:

Yellow   Noncluster-capable, but CDP-capable devices, or edge devices that are not running Cluster Management software. These devices are directly connected to a cluster member. Edge devices include Cisco switches, routers, hubs, or micro-web servers. Edge devices can only be Cisco devices.

Green   Cluster icon. A double-switch icon represents all members of the current cluster. Double-clicking the cluster icon launches the CVSM home page.

Blue   Candidate switches that are not part of the cluster but are eligible.

White   Additional clusters. If devices are directly connected to the cluster but are part of another cluster, these devices are represented by a double-switch icon as long as one of the devices connected is the command switch of the other cluster. If none of the devices connected is a command switch, they are all displayed as edge devices with yellow labels.

Table 2-9 describes the active buttons in Cluster View. Table 2-10 lists the menu options available when you right-click a device. Table 2-11 lists the menu options available when you right-click a link.

Table 2-9   Cluster View Buttons

Button	Action
Cluster Manager	Displays Cluster Manager.
Toggle Views	Toggles between Cluster Builder and Cluster View. In Cluster Builder, the command switch, members, and candidate switches are displayed.
Toggle Labels	Changes the labels on the links and icons. The labels can be • MAC address (IP address of the command switch) of the switch and the port numbers that connect links. A candidate switch also displays its IP addresses if one is assigned. • Host names.

Table 2-9   Cluster View Buttons (continued)

Button	Action
Save Layout	Saves the current layout of the switch icons. As long as there are no topology changes, the saved layout displays the next time you display Cluster View. For more information, see the "Arranging and Saving the Device Layout" section on page 4-16.

Table 2-10   Cluster View Device Menu Options

Menu Item	Action (available when you right-click a device)
Device web page	Displays the web management page for the device.
Disqualification code	Describes why the switch is not a cluster member or candidate.

Table 2-11   Cluster View Link Menu Options

Menu Item	Action (available when you right-click a link)
Link Graph	Displays the performance graph for the link. You can plot the link utilization percentage and the total packets, bytes, and errors recorded on the link. To display a link graph, one end of the link must be connected to a port on a cluster member that is a 2900 or 3500 XL switch. Links between Catalyst 1900 and 2820 switches, Catalyst 2820 and 2820 switches, or Catalyst 1900 and 1900 switches cannot be graphed. For more information, see the "Displaying Link Utilization Graphs" section on page 4-37.

Using Cluster Manager

Cluster Manager displays images of cluster switches that you can use to monitor and configure the devices. You can configure a cluster member on the port-, switch-, or cluster-level.

For port-level configuration, right-click a port (or several ports on the same switch while holding the **Ctrl** key) to display the port pop-up menu. Table 2-12 describes the items available from this menu.

Table 2-12   Cluster Manager Port Menu Items

Menu Item	Action (available when you right-click a port)
Port Configuration	Double-click a port, or click a port (or several ports on the same switch while holding the **Ctrl** key) to display the Port Configuration window. From this window, you can configure the status, speed, duplex, and Port Fast settings. For more information, see the "Configuring Ports" section on page 4-21.
Link Graph	Right-click a port that is green to display the performance graph for the link. You can plot the link utilization percentage and the total packets, bytes, and errors recorded on the link. This feature is not available on Catalyst 1900 and 2820 switches. For more information, see the "Displaying Link Utilization Graphs" section on page 4-37.

You can click the Mode button to change the port LED mode and display the speed and duplex settings of all switch ports. The LEDs display real-time information on the status and configuration of the ports.

For device-level configuration, right-click the switch chassis to display the device pop-up menu. Table 2-13 describes the items available from this menu.

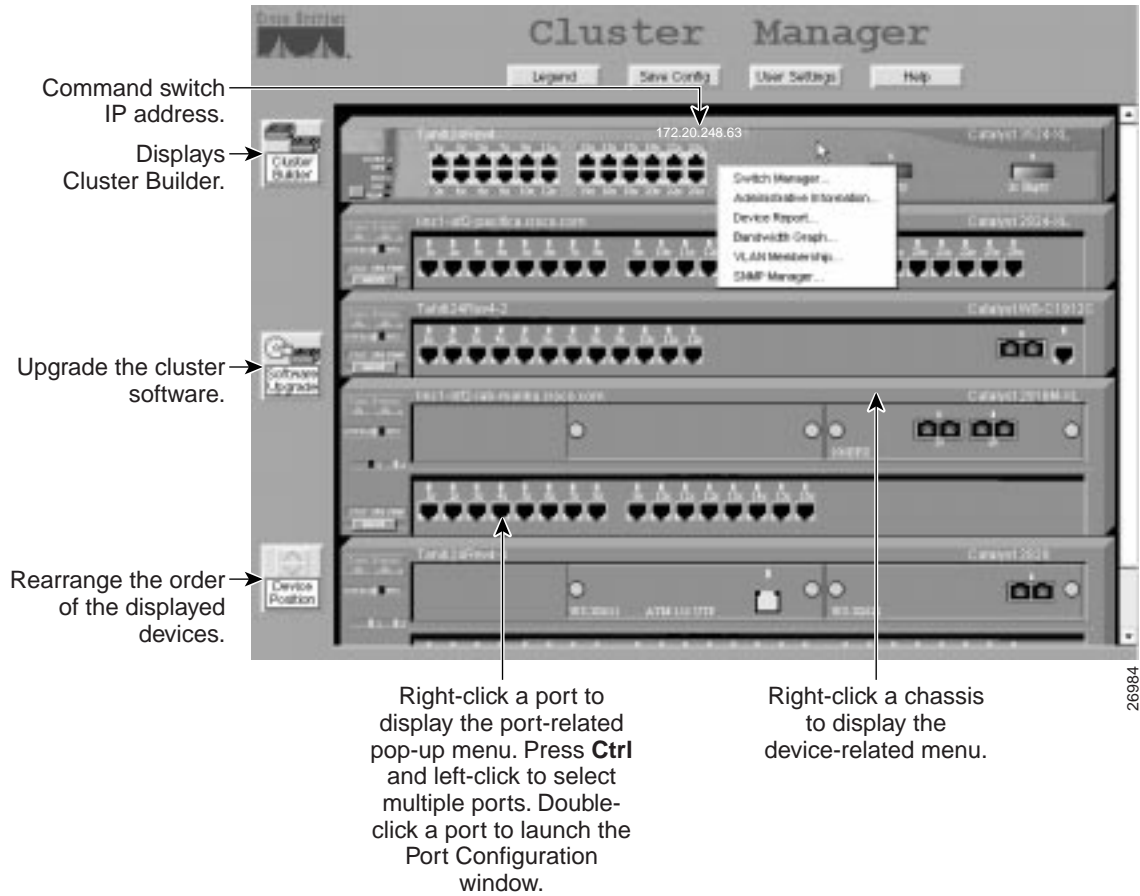**Table 2-13   Cluster Manager Device Menu Items**

Menu Item	Action (available when you right-click a switch chassis)
Switch Manager	Displays the switch manager home page. You can also display this page by double-clicking the command, member, or candidate switches. For more information, see the "Managing Your Switch through CVSM" section on page 3-14.
Administrative Information	Displays a window for entering the host name, system contact, and location. This window also displays the system uptime. The name you enter here is displayed on the switch in Cluster Manager and Cluster Builder. For more information, see the "Changing the Host Name" section on page 4-25.
Device Report	Displays the device report for the switch. The device report consists of three pages of information about the switch: configuration, system, and port. This feature is not available on Catalyst 1900 and 2820 switches. For more information, see the "Displaying Device Reports and Graphs" section on page 4-42.
Bandwidth Graph	Displays a graph that plots the total bandwidth in use by the switch. This feature is not available on Catalyst 1900 and 2820 switches. For more information, see the "Displaying Device Reports and Graphs" section on page 4-42.
VLAN Membership	Displays user configured VLANs on the switch. Select a VLAN, and click **Display Members** to show the ports that belong to the VLAN. Cluster Manager identifies the ports that belong to the selected VLAN by outlining them with a colored box on the switch image. Use the legend on the page to understand the VLAN port types. For more information, see the "Displaying VLAN Membership" section on page 4-26.
	The VLAN Membership menu option is not available on Catalyst 1900 or 2820 switches running standard edition software or running Enterprise Edition Software with bridge groups enabled.
SNMP Manager	Displays the window for configuring SNMP community strings and trap managers on cluster members. For more information, see the "Configuring SNMP" section on page 4-31.

For cluster-level configuration, click the buttons on the left side of the Cluster Manager window. Table 2-14 describes the group-level buttons.

Table 2-14   **Cluster Manager Cluster-Level Buttons**

Button Name	Action
Cluster Builder	Displays Cluster Builder.
Software Upgrade	Displays the window for performing group upgrades on cluster members. For more information, see the "Upgrading Software for a Group of Switches" section on page 4-27.
Device Position	Displays the window for rearranging the position of cluster members in Cluster Manager. By default, the command switch is displayed at the top of the stack of switches. For more information, see the "Rearranging the Order of the Switches" section on page 4-37.

Figure 2-7   Cluster Manager

Command switch
IP address.

Displays
Cluster Builder.

Upgrade the cluster
software.

Rearrange the order
of the displayed
devices.

Right-click a port to
display the port-related
pop-up menu. Press **Ctrl**
and left-click to select
multiple ports. Double-
click a port to launch the
Port Configuration
window.

Right-click a chassis
to display the
device-related menu.

Using the IOS Command-Line Interface

This section introduces the Cisco IOS command-line interface (CLI). The *Cisco IOS Desktop Switching Command Reference* (online only) contains a complete description of commands that have been created or changed for the 2900 and 3500 XL switches.

This section describes how to perform the following tasks:

- Understand the CLI and its command modes
- Use the CLI to manage member switches
- Set passwords
- Configure the switch for Telnet
- Work with files in Flash memory

Note When configuring your switch with the CLI, be aware that certain combinations of port features can create configuration conflicts. For more information, see the "Managing Configuration Conflicts" section on page 3-7.

Understanding the CLI

This section describes the Cisco IOS command-mode structure. Each command mode supports specific Cisco IOS commands. For example, the **interface** *type_number* command is used only from global configuration mode.

The switch supports the following command modes:

- User EXEC
- Privileged EXEC
- VLAN database (Enterprise Edition Software only)
- Global configuration
- Interface configuration
- Line configuration

Table 2-15 describes how to access each mode, the prompt you see in that mode, and how to exit the mode. The examples in the table use the host name *switch*.

Table 2-15   Command Modes Summary

Modes	Access Method	Prompt	Exit Method	About This Mode[1]
User EXEC	Begin a session with your switch.	`switch>`	Enter **logout** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	Enter the **enable** command while in user EXEC mode.	`switch#`	Enter **disable** to exit.	Use this mode to verify commands you have entered. Access to this mode should be protected with a password.

Table 2-15   Command Modes Summary (continued)

Modes	Access Method	Prompt	Exit Method	About This Mode[1]
VLAN database (Enterprise Edition Software only)	Enter the **vlan database** command while in privileged EXEC mode.	switch(vlan)#	To exit to privileged EXEC mode, enter **exit**.	Use this mode to configure VLAN-specific parameters.
Global configuration	Enter the **configure** command while in privileged EXEC mode.	switch(config)#	To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**.	Use this mode to configure parameters that apply to your switch as a whole.
Interface configuration	Enter the **interface** command (with a specific interface) while in global configuration mode.	switch(config-if)#	To exit to global configuration mode, enter **exit**. Press **Ctrl-Z** or enter **end** to return to privileged EXEC mode.	Use this mode to configure parameters for the Ethernet interfaces.
Line configuration	Specify a line with the **line vty** or **line console** command while in global configuration mode.	switch(config-line)#	To exit to global configuration mode, enter **exit**. Press **Ctrl-Z** or enter **end** to return to privileged EXEC mode.	Use this mode to configure parameters for the terminal line.

1   For any of the modes, you can see a comprehensive list of the available commands by entering a question mark (?) at the prompt.

Setting Passwords and Privilege Levels

Because many privileged EXEC commands are used to set operating parameters, you should password-protect these commands to prevent unauthorized use.

Catalyst 2900 and 3500 XL switches have two commands for setting passwords:

- **enable secret** *password* (a very secure, encrypted password)
- **enable password** *password* (a less secure, unencrypted password)

You must enter one of these passwords to gain access to privileged EXEC mode. It is recommended that you use the enable secret password.

If you enter the **enable secret** command, the text is encrypted before it is written to the config.text file, and it is unreadable. If you enter the **enable password** command, the text is written as entered to the config.text file where you can read it.

Note   When set, the enable secret password takes precedence, and the enable password serves no purpose.

Both types of passwords can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and both can start with a number. Spaces are also valid password characters; for example, *two words* is a valid password. Leading spaces are ignored; trailing spaces are recognized. The password is case sensitive.

To remove a password, use the **no** version of the commands: **no enable secret** or **no enable password**. If you lose or forget your enable password, see the "Recovering from a Lost or Forgotten Password" section on page 5-4.

When the Cluster Management software suggests a candidate to add to a cluster, you enter the password of the candidate switch, if one was defined, and the switch joins the cluster. Then the member switch inherits the command switch password. For more information on managing passwords in Cluster Management, see the "Changes to Passwords" section on page 4-10.

You can also specify up to 15 privilege levels and define passwords for them by using the **enable password** [**level** *level*] {*password*} or **enable secret** [**level** *level*] {*password*} command. Level 1 is normal EXEC-mode user privileges. If you do not specify a level, the privilege level defaults to 15 (traditional enable privileges).

Note You need privilege level 15 to access CVSM, Switch Network View, and the Cluster Management software. You must also use privilege level 15 if you configure TACACS+ (Enterprise Edition Software only) with the CLI so that all your HTTP connections will be authenticated through the TACACS+ server.

You can specify a level, set a password, and give the password only to users who need to have access at this level. Use the **privilege level** global configuration command to specify commands accessible at various levels. For more information on these commands, refer to the complete IOS Release 12.0 documentation set on CCO by selecting **Service and Support>Technical Documents>Documentation Home**.

Using the CLI to Manage Cluster Members

You can configure member switches with the CLI by first logging into the command switch. Enter the EXEC mode **rcommand** command and the member switch number to start a Telnet session (through a console or Telnet connection) and access the member switch CLI. Except when connecting to a Catalyst 1900 or 2820 switch running standard edition software with the command switch at privilege level 1 to 14, you are not prompted for a password because the member switch inherited the password of the command switch when it joined the cluster.

The following example shows how to log into member-switch 3 from the command-switch CLI:

```
switch# rcommand 3
```

If you do not know the member-switch number, enter the EXEC mode **show cluster members** command on the command switch.

For 2900 and 3500 XL switches, the Telnet session accesses the member-switch CLI at the same privilege level as on the command switch. The IOS commands then operate as usual. For instructions on configuring the 2900 or 3500 XL switch for a Telnet session, see the "Configuring the Switch for Telnet" section on page 2-36.

For Catalyst 1900 and 2820 switches running standard edition software, the Telnet session accesses the menu console (the menu-driven interface) if the command switch is at privilege level 15. If the command switch is at privilege level 14, you are prompted for the password before being able to access the menu console.

Command switch privilege levels map to the Catalyst 1900 and 2820 member switches running standard and Enterprise Edition Software as follows:

- If the command switch privilege level is 1 to 14, the member switch is accessed at privilege level 1.

- If the command switch privilege level is 15, the member switch is accessed at privilege level 15.

The Catalyst 1900 and 2820 CLI is available only on switches running Enterprise Edition Software.

Getting Help

You can use the question mark (?) and arrow keys to help you enter commands.

For a list of available commands in a command mode, enter a question mark:

```
switch> ?
```

To complete a command, enter a few known characters followed by a tab (with no space):

```
switch# sh conf<tab>
switch#sh configuration
```

For a list of command variables, enter the command followed by a space and a question mark:

```
switch> show ?
```

To redisplay a command you previously entered, press the up-arrow key. You can continue to press the up-arrow key for more commands.

Abbreviating Commands

You only have to enter enough characters for the switch to recognize the command as unique. This example shows how to enter the **show configuration** command:

```
switch# show conf
```

Using **no** Commands

The word *no* can be used to create a **no** form of a command. The **no** form of a command does the following:

- Resets a command to its default values.

  or

- Reverses the action of a command. For example, the command **no shutdown** reverses the shutdown of an interface.

Understanding Command-Line Error Messages

Table 2-16 lists some error messages that you might encounter while using the CLI to configure your switch.

Table 2-16   Common CLI Error Messages

Error Message	Meaning	How to Get Help
`% Ambiguous command: "show con"`	You did not enter enough characters for your switch to recognize the command.	Reenter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
`% Incomplete command.`	You did not enter all of the keywords or values required by this command.	Reenter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.

Table 2-16   Common CLI Error Messages (continued)

Error Message	Meaning	How to Get Help
`% Invalid input detected at '^' marker.`	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all of the commands that are available in this command mode.
		The possible keywords that you can enter with the command are displayed.

Configuring the Switch for Telnet

The following procedure describes one way to configure a Telnet password.

Task		Prompt	Command
Step 1	Attach a PC or workstation with emulation software to the switch console port.		
	The default data characteristics of the console port are 9600, 8, 1, no parity. When the command line appears, go to Step 2.		
Step 2	Enter privileged EXEC mode.	`switch>`	**enable**
Step 3	Enter global configuration mode.	`switch#`	**config terminal**
Step 4	Enter the interface configuration mode for the Telnet interface.	`switch(config)#`	**line vty 0 15**
	There are 16 possible sessions on a command-capable switch. The 0 and 15 indicate that you are configuring all 16 possible Telnet sessions.		
Step 5	Enter a password.	`switch(config)#`	**password** *password*
Step 6	Return to privileged EXEC mode so that you can verify the entry.	`switch(config)#`	**end**
Step 7	Display the running configuration.	`switch#`	**show running-config**
	The password is listed under the command **line vty 0 15**		
Step 8	(Optional) Save the running configuration to the startup configuration.	`switch#`	**copy running-config startup-config**

Starting a Telnet Session from the Browser

Follow this procedure to start a Telnet session by using a browser:

Step 1   Start one of the supported browsers.

Step 2   In the **URL** field, enter the IP address of the command switch.

Step 3   When the Cisco Systems Access page (Figure 2-1) is displayed, click **Telnet - to the switch** to start the Telnet session.

Working with Files in Flash Memory

You can use the file system in Flash memory to copy files and to troubleshoot configuration problems. Use 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 conffile.txt from the host arno to switch Flash memory with the name bootfile:

```
switch# copy tftp://arno//2900/conffile.txt flash:bootfile
```

You can enter the following parameters as part of a filename:

- TFTP

- Flash

- RCP

- XMODEM

Use the **copy running-config startup-config** 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#
```

Using SNMP Management

This section describes how to access Management Information Base (MIB) objects to configure and manage your switch. It provides the following information:

- Using FTP to access the MIB files

- Using SNMP to access the MIB variables

Note   When configuring your switch using SNMP, be aware that certain combinations of port features create configuration conflicts. For more information, see the "Preparing to Use the Web-Based Management Interfaces" section on page 2-2.

Using FTP to Access the MIB Files

You can obtain each MIB file with the following procedure:

Step 1   Use FTP to access the server **ftp.cisco.com**.

Step 2   Log in with the username **anonymous**.

Step 3   Enter your e-mail username when prompted for the password.

Step 4   At the `ftp>` prompt, change directories to **/pub/mibs/supportlists**.

Step 5   Change directories to one of the following:

- **wsc2900xl** for a list of 2900 XL MIBs

- **wsc3500xl** for a list of 3500 XL MIBs

Step 6   Use the **get** *MIB_filename* command to obtain a copy of the MIB file.

Using SNMP to Access MIB Variables

The switch MIB variables are accessible through SNMP, an application-layer protocol facilitating the exchange of management information between network devices. The SNMP system consists of three parts:

- The SNMP manager, which resides on the network management system (NMS)

- The SNMP agent, which resides on the switch

- The MIBs that reside on the switch but can be compiled with your network management software

An example of an NMS is the CiscoWorks network management software. CiscoWorks software uses the switch MIB variables to set device variables and to poll devices on the network for specific information. The results of a poll can be displayed as a graph and analyzed in order to troubleshoot internetworking problems, increase network performance, verify the configuration of devices, monitor traffic loads, and more.

As shown in Figure 2-8, the SNMP agent gathers data from the MIB, which is the repository for information about device parameters and network data. The agent can send traps, or notification of certain events, to the SNMP manager, which receives and processes the traps. Traps are messages alerting the SNMP manager to a condition on the network
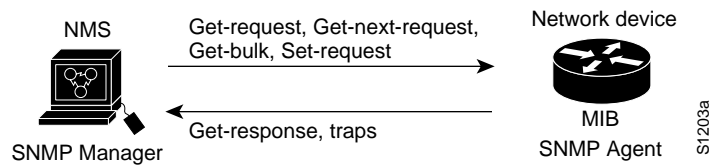
such as improper user authentication, restarts, link status (up or down), and so forth. In addition, the SNMP agent responds to MIB-related queries sent by the SNMP manager in *get-request*, *get-next-request*, and *set-request* format.

The SNMP manager uses information in the MIB to perform the operations described in Table 2-17.

Figure 2-8   SNMP Network

Table 2-17   SNMP Operations

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves a value from a variable within a table.[1]
get-response	Replies to a get-request, get-next-request, and set-request sent by an NMS.
set-request	Stores a value in a specific variable.
trap	An unsolicited message sent by an SNMP agent to an SNMP manager indicating that some event has occurred.

1   With this operation, an SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.

Managing Clusters through SNMP

SNMP must be enabled for the Cluster Management reporting and graphing features to function properly. When you power-up your 2900 or 3500 XL switch for the first time, SNMP is enabled if you enter the IP information by using the setup program and accept its proposed configuration. If you did not use the setup program to enter the IP information, and SNMP was not enabled, you can enable it on the SNMP Configuration page described in the "Configuring SNMP" section on page 3-59. On Catalyst 1900 and 2820 switches, SNMP is enabled by default.

When a cluster is created, the command switch manages the exchange of messages between member switches and an SNMP application. The Cluster Management software appends the member switch number (@*esN*, where *N* is the switch number) to the first configured RW and RO community strings on the command switch and propagates them to the member switch. The command switch uses this community string to control the forwarding of gets, sets, and get-next messages between the SNMP management station and the member switches. The command switch also passes traps from the member switch to the management station, as shown in Figure 2-9, if the member switch does not have an IP address. If a member switch has its own IP address and community strings, they can be used in addition to the access provided by the command switch. For more information, see the "Changes to the SNMP Community Strings" section on page 4-9 and the "Configuring SNMP" section on page 4-31.

Figure 2-9 **SNMP Management for a Cluster**