

Using the Management Interfaces

This chapter describes the features and management characteristics of the management interfaces. You can use these interfaces to monitor and configure a switch or a group of switches.

There are three web-based management tools that you access via a browser such as Netscape Navigator or Microsoft Internet Explorer:

- Cisco Visual Switch Manager (CVSM) for managing a switch
With CVSM, you can configure a switch via a graphical user interface and monitor live images of the switch.
- Switch Network View 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.
- Cluster Management 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.

There are two other interfaces you can use to manage a switch or group of switches:

- Cisco IOS software, a command-line interface (CLI) accessed via the console port or Telnet
- SNMP MIB objects accessed via an SNMP management application

Table 3-1 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 site 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.

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 an HTML session to ensure that the browser is supported. If the browser is not supported, the switch displays an error message, and the HTML 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 only display edge devices connected to the command switch. Other functionality is similar to that of Netscape Communicator.

The following operating systems are supported for HTML management:

- Windows 95 Service Pack 1
- Windows 98
- Windows NT (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 the HTML Interfaces

Browser	Minimum Version	Supported Versions
Netscape Communicator	4.5	4.5, 4.51
Microsoft Internet Explorer	4.01a	4.01, 5.0

Table 2-2 lists the configuration that yields the best results for the HTML interfaces.

Table 2-2 Recommended Platform Configuration for the HTML Interfaces

OS	Processor Speed	DRAM	Number of Colors	Resolution	Font Size
WindowsNT	Pentium 300 MHz	128 MB	65536	1024x768	Small

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 **Advanced**.
- (a) Scroll through the list of options until you see Java VM. Select the **Java JIT compiler enabled** and **Java logging enabled** check boxes.
 - (b) Click **Apply**.
 - (c) Click **General**. In the Temporary Internet Files section, click **Settings**. The Settings window opens.
- Step 4** Click **Every visit to the page**, and click **OK**.
- Step 5** In the Internet Options window, click **Security**.
- (a) In the Zone drop-down list, select **Trusted Sites Zone**.
 - (b) In the Trusted Sites Zone section, click **Custom**.
 - (c) Click **Settings**.
- Step 6** Select **Java>Java Permissions** section, and select **Custom**.
Click **Java Custom Setting**, which appears at the bottom of the window.
- Step 7** In the Trusted Sites Zone window, click **Edit Permissions**.
- (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 **Security**.
- (a) Verify that the Zone drop-down list is set to **Trusted Sites Zone**.
 - (b) In the Trusted Sites Zone section, click **Add Sites**.

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 cluster command switch, as in this example:

http://172.20.153.36

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

Note You do not need to enter the IP addresses of member switches. However, if a switch does have an IP address and you want to leave open the possibility of direct management, enter the member switch IP address as you did the command switch IP address.

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

Configuring Microsoft Internet Explorer 5.0

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 **Security**.

Step 4 Select the **Trusted Sites** icon and click **Sites....**

Step 5 Deselect the **Require server verification** checkbox and click **Add**.

Step 6 Add the switches you want to manage by entering their URLs in the **Add this web site to the zone** field. A URL is the switch IP address preceded by **http://**.

Step 7 After you have finished entering the URLs for your switches, click **OK**.

Step 8 Still in the Security tab of Internet Options, click **Custom Level...**

Step 9 In the **Security Settings** dialog box, scroll down to the **Java>Java permissions** section.

- Step 10** Select **Custom**. This enables the **Java Custom Settings** button.
- Step 11** Click **Java Custom Settings** and then select **Edit Permissions**.
- Step 12** Under Run Unsigned Content, click **Enable**, and click **OK**.
- Step 13** Click OK to close the **Security Settings** dialog box.

Using Cisco Visual Switch Manager

CVSM is a web-based device-management site for configuring and monitoring your switch. Because the switch is preconfigured, CVSM pages show 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 a live image of the switch (see 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 3-31.

Accessing CVSM for the First Time

The switch must have an IP address before you can access CVSM. For instructions on assigning the IP address, see the “CLI Commands for Assigning IP Information to the Switch” section on page 3-42. Follow these steps to access CVSM:

- Step 1** Be sure that you have configured your browser correctly. See the “Preparing to Use the Web-Based Management Interfaces” section on page 2-2 for more information.
- 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**. The Cisco Systems Access page (see Figure 2-1) is displayed.
- Step 5** Click **Visual Switch Manager** to display the CVSM Home page, shown in Figure 3-4.

Figure 2-1 Cisco Systems Access Page

Cisco Systems

Accessing Cisco WS-C2912-XL "Switch202"

[Visual Switch Manager](#) - Manage the Switch through the web interface. ← Click here to display CVSM.

[Telnet](#) - To the Switch. ← Click here to open a Telnet session to the switch.

[Show interfaces](#) - Display the status of the interfaces.

[Show diagnostic log](#) - Display the diagnostic log.

[Web Console](#) - Display the HTML command line interface.

[Show tech-support](#) - Display information commonly needed by tech support.

[Cluster Management](#) - Manage the Cluster through the web interface. ← Click here to display Cluster Management.

Help resources

1. [CCO at www.cisco.com](http://www.cisco.com) - Cisco Connection Online, including the Technical Assistance Center (TAC).
 2. tac@cisco.com - e-mail the TAC.
 3. **1-800-553-2447** or **+1-408-526-7209** - phone the TAC.
 4. cs-html@cisco.com - e-mail the HTML interface development group.
- ← How to contact Cisco Systems.

22320

The CVSM Home page displays when you click **Visual Switch Manager** on the 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 described in Figure 2-2.

The other web-based tools are available from the CVSM Home page. Depending on your network, you can click **Cluster Management** to create and manage clusters of switches or **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.

Legend:

Status:	No Link Status	Link Up	Link Faulty or Port Disabled
Speed:	10 Mbps or No Link Status	100 Mbps or greater	
Duplex:	Half Duplex or No Link Status	Full Duplex	

Connect to Cisco Systems

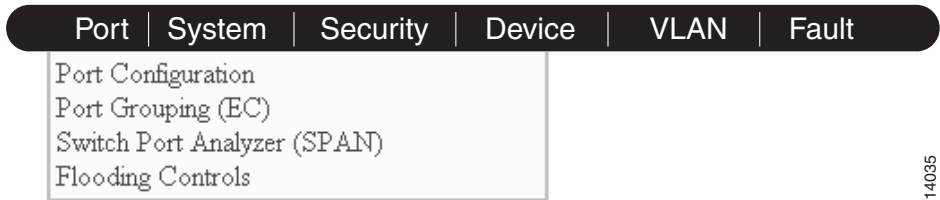
All contents copyright © 1997-1999 by Cisco Systems, Inc.

22340

CVSM Menu Options

You can access the device-management features of this release from the Home page 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



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 via Trivial File Transfer Protocol (TFTP).
System Time Management	Configure the time on the switch, or configure the switch to receive the time from an Network Time Protocol (NTP) server.
IP Management	Enter IP information for the switch.
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 addresses and the address aging time.
Port Security	Enable port security.
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 the Network View, you can display switch-connection information, device reports, and link reports.

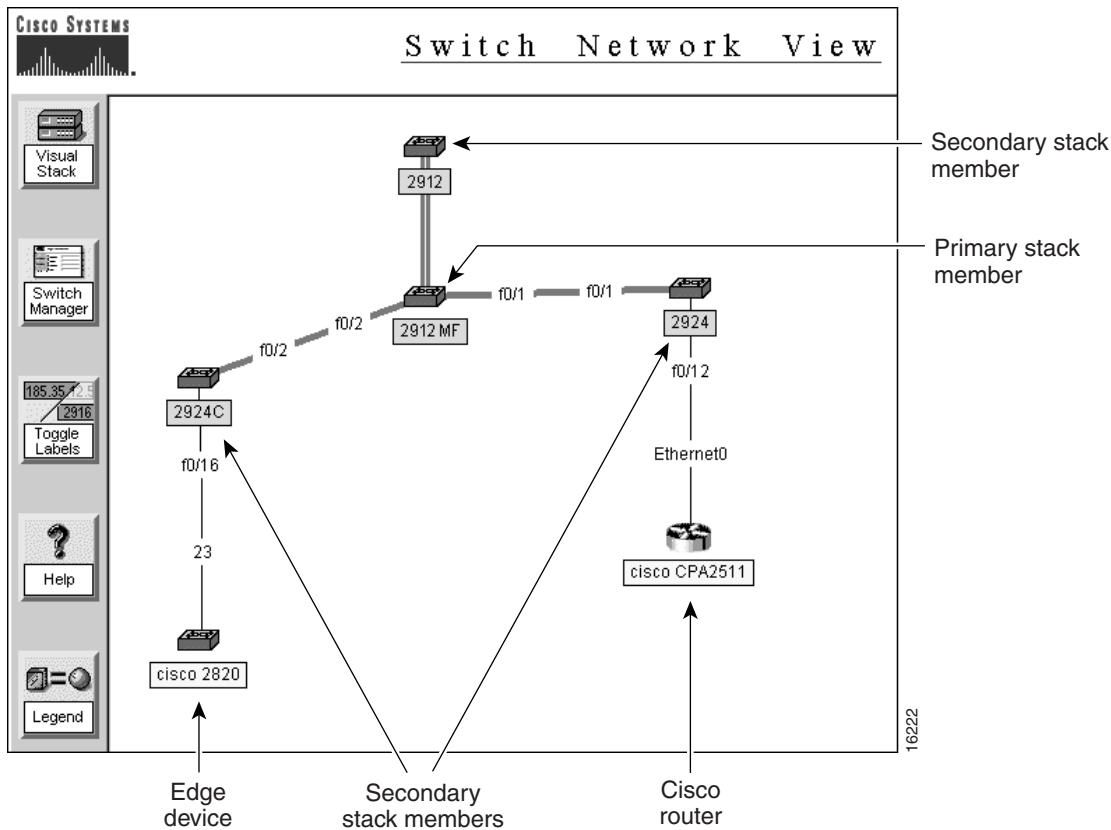
You display Network View from the switch home page, but its availability depends on how your switch is configured. If your switch is part of a cluster, the button displays **Cluster Management**. If it is not part of a cluster, the button displays **Switch Network View**.

If your switch is not in a cluster, click **Switch Network View** on the CVSM Home page to display the view shown in Figure 2-4. Blue labels identify stack members. Yellow labels identify generic edge devices connected to stack members. Network View can also display Cisco routers, switches, hubs, and Cisco Micro Webservers if they are directly attached to a switch running IOS Release 11.2(8)SA6 or later.

Table 2-4 Network View Buttons

Name	Purpose
Visual Stack	Display live images of stack members. From this page you can: <ul style="list-style-type: none"> • Display the status, duplex, speed and Port Fast settings on this port. • Configure ports. • Start the CVSM for any stack member.
Switch Manager	Display 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	Alternate between displaying IP addresses and device type labels.
Help	Display online help.
Legend	Display the meanings of icons and links.

Figure 2-4 Switch Network View Page



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 information, system information, and information about individual ports. |
| Switch Manager | Displays the CVSM Home page for the switch. |

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 STP state.

Using Cluster Management

Cluster Management consists of three related tools that you can use to create clusters of switches, manage individual switches, and display device information, link information, and performance graphs. This section describes how you can use the following Cluster Management tools to manage your network:

- Cluster Builder
- Cluster View
- Cluster Manager

Accessing Cluster Management

See the “Creating Clusters” section on page 4-2 for information on how to create a cluster.

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

- Click Cluster Management on the switch Home page
- Click Cluster Management on the Cisco Access page, as shown in Figure 2-1.

Common Interface Features in Cluster Management

Certain features are common to all three Cluster Management tools. 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 of cluster switches to permanent storage. These configurations are saved in the config.text file that is used when the switches are reset. For more information, see the “Working with Files in Flash Memory” section on page 2-31.
User Settings	Configure 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: <ul style="list-style-type: none">• 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
Help	Displays detailed procedures for Cluster Management tasks.

Using Cluster Builder

Use Cluster Builder to automatically or manually create a cluster of switches. Devices directly connected to the command switch and running the appropriate software display in color to identify them 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). After the cluster is created, you can collapse the entire cluster into a single icon by clicking **Toggle Views** to display Cluster View. 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. Add these candidates to the cluster with Cluster Builder.

Yellow A directly connected Cisco device that cannot be a cluster member. These can be routers, hubs, switches, or other Cisco devices.

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 it is a cluster member or not.

Figure 2-5 Cluster Builder

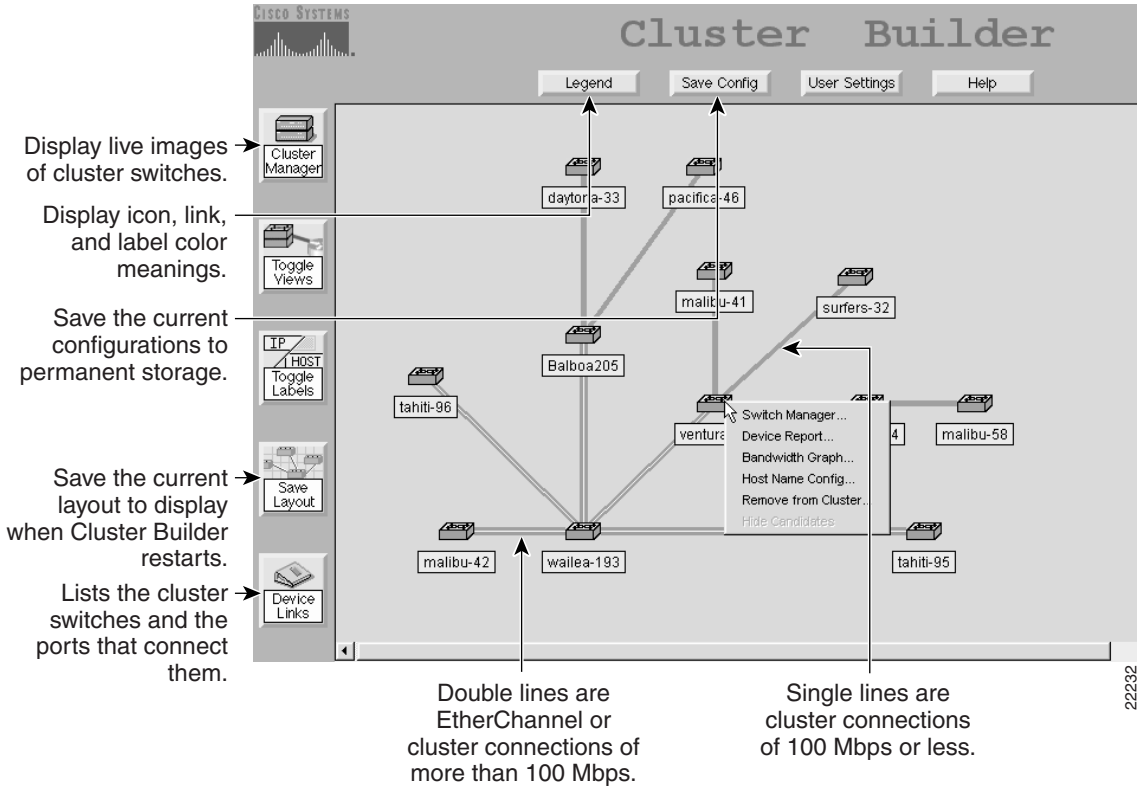


Table 2-6 Cluster Builder Buttons

Button	Action
Cluster Manager	Displays the Cluster Manager page.
Toggle Views	Toggles between Cluster View and Cluster Builder. In Cluster View, all cluster switches are represented by a single icon.
Toggle Labels	Changes the labels on the links and icons. The labels can be <ul style="list-style-type: none">• IP or MAC addresses for the switches and the port numbers that connect them.• Host names.
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.
Device Links	Lists the switches and the ports that connect them.

Table 2-7 Cluster Builder Device Menu Items

Menu Item	Action
Switch Manager	Displays the switch CVSM Home page.
Device Report	Displays the device report for the switch. The device report has three pages of information about the switch: configuration information, system information, and port information.
Bandwidth Graph	Displays a graph that plots the total bandwidth used by the switch.
Host Name Config	Displays a window where you can enter a host name for the switch.
Device Web Page	Displays the HTML interface for the device. (Not always displayed.)
Add to Cluster	Adds the selected switch to the cluster. (Not always displayed.)
Remove from Cluster	Removes the selected switch from the cluster. (Not always displayed.)
Hide Candidates, Show Candidates	Hides or redisplay candidate switches.

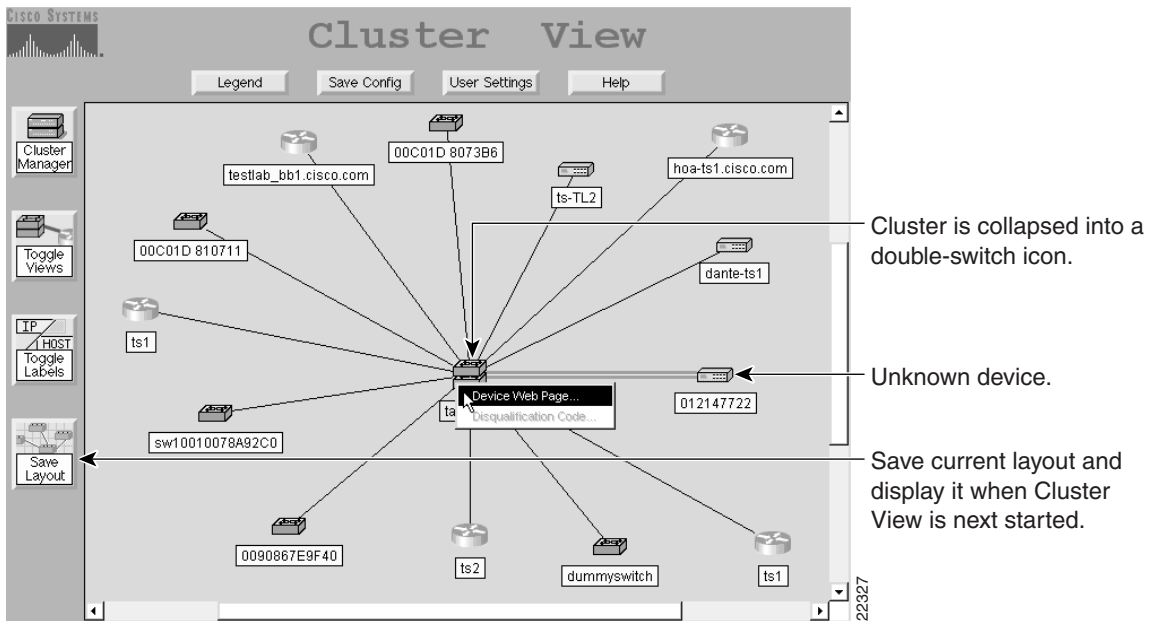
Table 2-8 Cluster Builder Link Menu Items

Menu Item	Action
Link Report	Displays the link report for the link. This report displays the link speed, VLAN and port group memberships, and STP state. You can display the link graphs from this report.
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.

Using Cluster View

Cluster View displays the cluster as a single icon and edge devices and candidate switches connected to the cluster. 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	Edge devices that are not running Cluster Management software
Green	Cluster icon
Blue	Candidate switches that are not qualified for membership
White	Additional clusters

Table 2-9 lists the menu options available when you right-click a device. Table 2-10 lists the menu options available when you right-click a link.

Table 2-9 Cluster View Device Menu Options

Menu Item	Action
Device web page	Displays the CVSM Home page for Catalyst 2900 XL and Catalyst 3500 XL switches.
Disqualification code	Describes why the switch is not a cluster member or candidate.

Table 2-10 Cluster View Link Menu Options

Menu Item	Action
Link Report	Displays the speed and duplex settings for the link, the STP state, port group memberships, and the VLANs the ports belong to.
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.

Using Cluster Manager

Cluster Manager displays live images of cluster switches that you can use to monitor and configure the devices. You can click a port, or several ports, to configure status, speed, duplex and Port Fast settings.

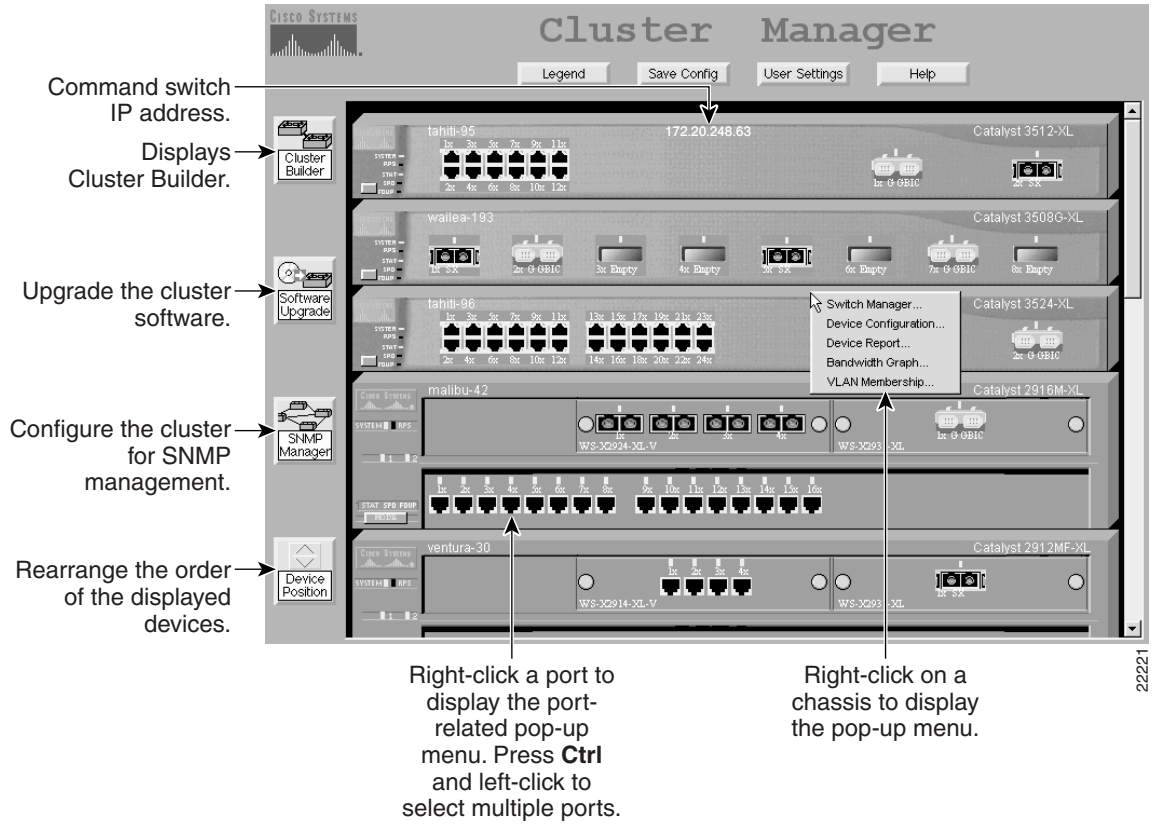
The LEDs display real-time information on the status and configuration of the ports. Click the Mode button to change the port LED mode to display the speed and duplex settings of all switch ports. Click **Device Position** to place the images in any order.

Click a switch chassis and right-click to display the device pop-up window. Table 2-11 describes the items available from this menu.

Table 2-11 Cluster Manager Device Menu Items

Menu Item	Action
Switch Manager	Displays the switch CVSM Home page.
Device Configuration	Displays a dialog box for entering the host name, system contact, location, and system-up time. The name you enter here is displayed on the switch in Cluster Manager and Cluster Builder. The system-up time is also displayed.
Device Report	Displays the device report for the switch. The device report consists of three pages of information about the switch: configuration information, system information, and information about individual ports.
Bandwidth Graph	Displays a graph that plots the total bandwidth in use by the switch.
VLAN Membership	Displays a dialog box that displays all VLANs configured on the switch. Select a VLAN, and click Display Members to show the ports that belong to the VLAN. Use the legend on the page to understand the VLAN port types.

Figure 2-7 Cluster Manager



22221

Using the IOS Command-Line Interface

This section introduces the Cisco IOS command-line interface (CLI). The *Cisco IOS Desktop Switching Command Reference: Catalyst 2900 Series XL and Catalyst 3500 Series XL Cisco IOS Release 11.2(8)SA6* is a complete description of commands that have been created or changed for the switches. The documentation set for Cisco IOS Release 11.2(8) describes the other command 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 using 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 3-5.

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 2-12 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 2-12 Command Modes Summary

Modes	Access Method	Prompt	Exit Method	About This Mode ¹
User EXEC	Begin a session with your switch.	switch>	Enter the logout command or quit .	Use this mode to <ul style="list-style-type: none">• Change terminal settings.• Perform basic tests.• Display system information.
Privileged EXEC	Enter the enable command while in user EXEC mode.	switch#	Enter the disable command to exit.	Use this mode to verify commands you have entered. Access to this mode should be protected with a password.

Table 2-12 Command Modes Summary (continued)

Modes	Access Method	Prompt	Exit Method	About This Mode¹
VLAN database (Enterprise Edition Software only)	Enter the vlan database command while in privileged EXEC mode.	<code>switch(vlan) #</code>	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.	<code>switch(config) #</code>	To exit to privileged EXEC mode, enter the exit or end command, 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.	<code>switch(config-if) #</code>	To exit to global configuration mode, enter the exit command. 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.	<code>switch(config-line) #</code>	To exit to global configuration mode, enter the exit command. 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.

Using the CLI to Manage Cluster Members

You can configure member switches via the CLI by first logging in to the command switch. Enter the EXEC mode **rcommand** command and the number of the member switch to access the member switch CLI. The following example shows how to log in to 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. When you display the member-switch CLI, the command mode changes and the IOS commands then operate as usual.

See the “Starting a Telnet Session from the Browser” section on page 2-30 for instructions on starting a Telnet session to the switch.

Setting Passwords

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

There are 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 commands to gain access to privileged EXEC mode. It is recommended that you use the **enable secret** command.

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

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.

When Cluster Management suggests a candidate to add to a cluster, there is a field where you can enter the enable password of the candidate. If you enter the password that has already been defined for the candidate, the switch joins the cluster and then inherits the enable password of the command switch. See the “Automatically Discovering Cluster Candidates” section on page 4-4 for more information on managing enable passwords in Cluster Management.

To unset a password, use the **no** version of the commands: **no enable password** or **no enable secret**.

If you lose or forget your enable password, see the “Recovering from a Lost or Forgotten Password” section on page 5-4.

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 2-13 lists some error messages that you might encounter while using the CLI to configure your switch.

Table 2-13 Common CLI Error Messages

Error Message	Meaning	How to Get Help
<code>% Ambiguous command: "show con"</code>	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.
<code>% Incomplete command.</code>	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.
<code>% Invalid input detected at '^' marker.</code>	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 password for Telnet.

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. There are 16 possible sessions on a command-capable switch. The 0 and 15 indicate that you are configuring all 16 possible Telnet sessions.	switch(config)#	line vty 0 15
Step 5 Enter a password.	switch(config)#	password <i>password</i>
Step 6 Return to privileged EXEC mode so that you can verify the entry.	switch(config)#	end
Step 7 Display the running configuration. The password is listed under the command line vty 0 15 .	switch#	show running-config
Step 8 As an option, 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 via 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 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#
```

SNMP Management

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

- MIB file list
- Using FTP to access the MIB files
- Using CCO 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.

MIB Files

The MIB files contain variables that can be set or read to provide information about the switch, such as the traps generated by the switch.

The following MIB files contain the MIB and trap information for the switch:

- RFC1213-MIB.my contains the MIB II (RFC 1213).
- CISCO-C2900-MIB.my contains the device-specific MIB.
- BRIDGE-MIB.my contains the bridge MIB (RFC 1493).
- CISCO-CDP-MIB-V1SML.my contains the Cisco Discovery Protocol (CDP) MIB.
- CISCO-VLAN-MEMBERSHIP-MIB.V1SML.my controls VLAN membership of ports.
- CISCO-SWITCH-CGMP-MIB.my controls Cisco Group Management Protocol.

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**.
- Step 5** Use the **get README** command to display the readme file containing a list of available files.
- Step 6** Use the **get MIB_filename** command to obtain a copy of the MIB file.

Using CCO to Access the MIB Files

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: `cco.cisco.com`
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

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: SNMP manager, SNMP agent, and MIB.

Instead of defining a large set of commands, SNMP places all operations in a *get-request*, *get-next-request*, and *set-request* format. For example, an SNMP manager can get a value from an SNMP agent or store a value into that SNMP agent. The SNMP manager can be part of a network management system (NMS), and the SNMP agent can reside on a networking device such as a switch. You can compile the switch MIB files with your network management software. The SNMP agent can respond to MIB-related queries being sent by the NMS.

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 manager.

The SNMP manager uses information in the MIB to perform the operations described in Table 2-14.

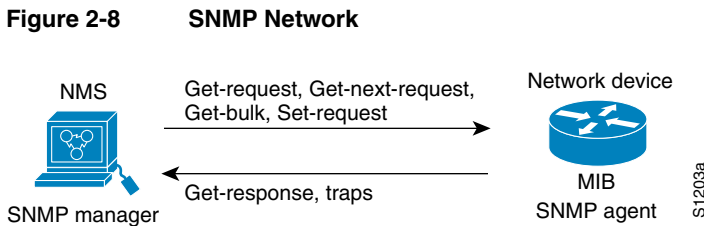


Table 2-14 **SNMP Operations**

Operation	Description
get-request	Retrieve a value from a specific variable.
get-next-request	Retrieve a value from a variable within a table. ¹
get-response	The reply to a get-request, get-next-request, and set-request sent by an NMS.
set-request	Store 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 via SNMP

SNMP must be enabled for the Cluster Management reporting and graphing features to function properly. When you power-up your switch for the first time, SNMP is enabled if you enter the IP information via 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 page described in the “Disabling and Enabling SNMP” section on page 3-43.

When a cluster is created, the command switch manages the exchange of messages between member switches and an SNMP application by appending the host name of the member switch to the first configured RW and RO community strings. The command switch uses this community string to control the forwarding of messages, such as traps, between the SNMP management station and the member switches, as shown in Figure 2-9. However, 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.

Figure 2-9 SNMP Management for a Cluster

