Using the Management Interfaces

This chapter describes the features and characteristics of the management interfaces available on the 2900 and 3500 XL switches. There is a command-line interface for entering IOS commands, a graphical user interface (GUI) for use with a browser such as Microsoft Internet Explorer or Netscape Navigator, and an Simple Network Management Protocol (SNMP) interface for SNMP management applications such as CiscoWorks2000 and CiscoView 5.0.

This chapter describes the following topics:

- Configuring your management station to use the Cluster Management Suite (CMS), the HTML-based interface for configuring clusters and individual switches

- Understanding the menu options, icons, and other graphical devices that make up the CMS interface

- Understanding how to change command modes and enter commands by using the IOS command-line interface (CLI)

- Understanding how to use an SNMP management application to manage a cluster or switch

Note If you are looking for information on a specific feature, Table 4-2 on page 4-3 lists the defaults for all key features and provides cross-references to feature descriptions and CLI procedures.

Preparing to Use Cluster Management Suite

All of the CMS features are based on an embedded HTTP web server in the switch Flash memory. Follow these steps to prepare to use CMS:

1. Ensure that your system meets the required specifications listed in this section.

2. Follow the steps in the "Installing the Required Plug-In" section on page 2-3.

3. Configure your browser as described in this section.

Web-based management uses HTTP, an in-band form of communication: you access the switch through one of its Ethernet ports. Therefore, do not disable or otherwise misconfigure the port through which *you* are communicating with the switch.

You access CMS through the default privilege level 15. For more information, see the "Setting Passwords and Privilege Levels" section on page 2-34.

Hardware and Software Requirements

The minimum requirement for a PC is a Pentium processor running at 233 MHz with 64 MB of DRAM. The minimum requirement for a UNIX workstation is a Sun Ultra 1 running at 143 MHz with 64 MB of DRAM. Table 2-2 lists the recommended platforms.

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	4.61[1]	4.61, 4.7
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.

Note   In Cluster Management, Internet Explorer versions 4.01 and 5.0 do not display edge devices that are not connected to the command switch. Other functionality is similar to that of Netscape Communicator.

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
Solaris 2.5.1	Sparc 333 MHz	128 MB	Most colors for applications	—	Small (3)

Installing the Required Plug-In

A browser plug-in is required to access CMS. You can download the plug-in from Cisco Connection Online (CCO).

If you have a SmartNet support contract, you can login to one of the following URLs and download the plug-in:

```
http://www.cisco.com/cgi-bin/tablebuild.pl/cat2900XL
http://www.cisco.com/cgi-bin/tablebuild.pl/cat3500XL
```

If you do not have a SmartNet contract, you can download the plug-in from one of the following URLs:

```
http://www.cisco.com/pcgi-bin/tablebuild.pl/cat2900XL
http://www.cisco.com/pcgi-bin/tablebuild.pl/cat3500XL
```

Follow the instructions that accompany the plug-in to install it on your computer.

After you have installed the plug-in, you can access the CMS 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.

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**.

Step 4   Select the **Enable Java**, **Enable JavaScript**, and **Enable Style Sheets** check boxes.

Step 5   From the menu bar, select **Edit>Preferences**.

Step 6   In the Preferences window, click **Advanced Cache**, and select **Every time**.

Step 7   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

To manage a cluster, add the IP address of the command switch. To manage a cluster that has Hot Standby Router Protocol (HSRP) enabled, enter the virtual IP address of the cluster.

If you plan to use Visual Switch Manager (VSM) for switch configuration, you 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 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** To manage a cluster, add the IP address of the command switch. To manage a cluster that has HSRP enabled, enter the virtual IP address of the cluster.
>
> If you plan to use VSM for switch configuration, 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, note that this browser does not automatically reflect the latest configuration changes. Make sure you click the browser **Refresh** button for every configuration change.

Using the Cluster Management Suite

The Cluster Management Suite consists of four related applications that you can use to create clusters of switches, monitor and configure switches and ports, and display link and performance information. Each cluster requires a designated command switch with an IP address to manage communication with the other switches in the cluster.

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

- Cluster Builder
- Cluster View
- Cluster Manager
- Visual Switch Manager (VSM)

These CMS applications support the monitoring and configuration of all cluster and switch features. VSM provides monitoring and configuration of all device-management features for standalone switches.

All CMS applications are supported by an online help system.

Accessing CMS for the First Time

Use the IP address of a cluster command switch or standalone switch to access the appropriate web-based application. For instructions on assigning the IP address, see the "CLI: Assigning IP Information to the Switch" section on page 4-31. For information on clustering, see Chapter 3, "Creating and Managing Clusters."

If your network is configured with an HSRP standby group for redundancy, enter the *virtual* IP address to access CMS. See the "Building a Redundant Cluster" section on page 3-17 for more information.
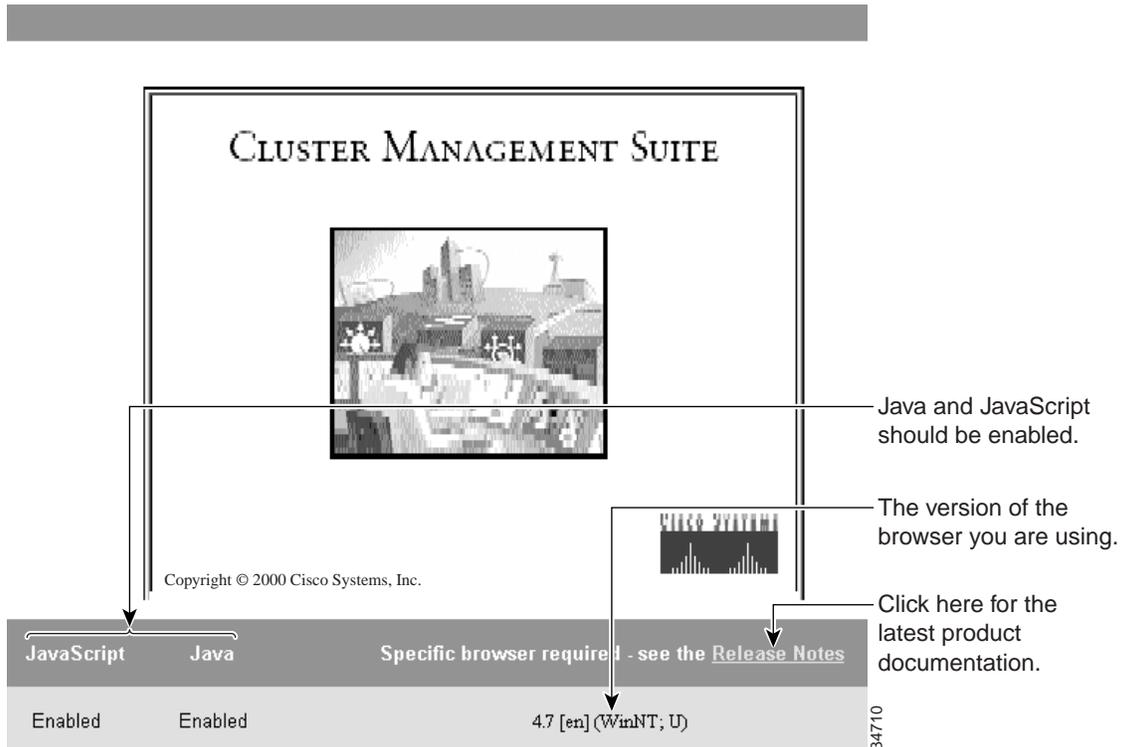
Follow these steps to access Cluster Management:

Step 1   Start the browser.

Step 2   Be sure that the browser is configured correctly. See the "Preparing to Use Cluster Management Suite" section on page 2-2 for details on configuring the browser.

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

Step 4   Enter your username and password when prompted. The password provides level 15 access. The Cisco Systems Access page (Figure 2-1) is displayed.

Step 5   Click **Cluster Management Suite or Visual Switch Manager** to display the appropriate CMS application.

Figure 2-1   Cisco Systems Access Page
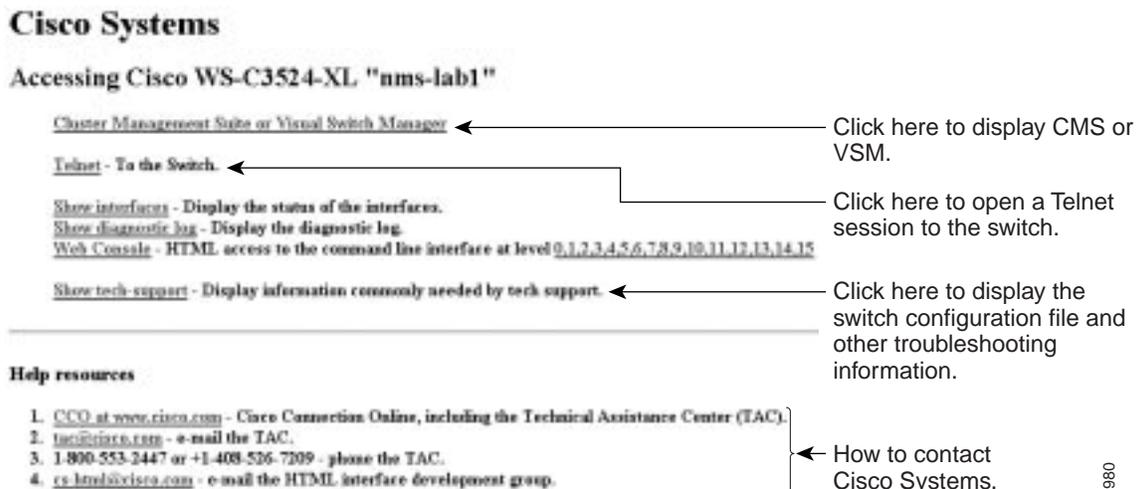
A *splash* screen (Figure 2-2) displays momentarily before the application. Depending on how you have CMS configured, Cluster Builder or Cluster Manager then displays.

Figure 2-2   Cluster Management Suite Splash Screen

Java and JavaScript should be enabled.

The version of the browser you are using.

Click here for the latest product documentation.

Using CMS Windows

CMS windows use consistent techniques to present and save configuration information. In some cases, CMS windows have multiple *tabs* that present different kinds of information. Tabs are arranged like folder headings across the top of the window. Click the tab to display a new screen of information, and use the Apply button to save information on all tabs without closing the window.

When you are managing a cluster of switches, a drop-down Device List at the top of the window displays the names of all cluster switches. The contents of this list can vary depending on the menu item selected. For example, the VLAN Membership window would not display 1900 and 2820 switches, even though they are part of the cluster. Click on a switch to display the information for that switch. VSM windows, which always operate on a single switch, do not display a Device List.

Listed information can often be changed by selecting an item from a list. To change the information, select one or more items, and click **Modify**. Changing multiple items is limited to those items that apply to at least one of the selections. For example, when you select multiple ports, a parameter such as flow control is grayed out if the ports are not Gigabit Ethernet ports.

Tips   If you try to select a port or device in Cluster Manager while there is another window still open, the computer issues a ringing bell sound. Rearrange the windows that are displayed to find the open window, and close it to proceed.

Figure 2-3 shows the components of a typical CMS window.

The following are the most common buttons that you use to control a CMS window:

Button	Description
OK	Save any changes made in the window and close the window.
Apply	Save any changes made in the window and leave the window open.
Cancel	Do not save any changes made in the window and close the window.
Modify	Display the pop-up for changing information on the selected item or items. You usually select an item from a list or table and click **Modify**. When you close the pop-up, you return to the original window.
Help	Display the online help for the current window and the online help table of contents.

Figure 2-3   Components of a CMS Window
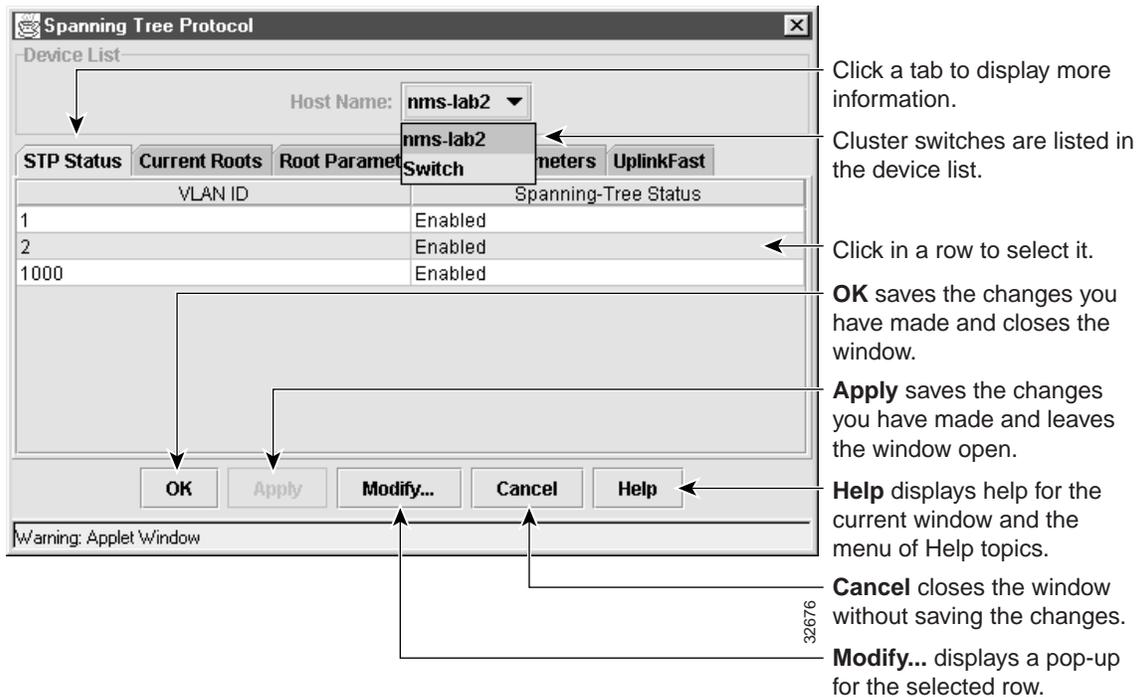
The Common Interface of Cluster Builder and Cluster View

Cluster Builder and Cluster View are related applications that share the same interface. Use Cluster Builder to create and modify clusters of switches and to display a network map of their links and devices. You can create clusters with redundant command switches and display cluster members and the links between them. Cluster View displays a map of the switches in a cluster and the neighboring edge devices and clusters. Once you have displayed Cluster Builder or Cluster View, you can toggle back and forth between the two.

The user interface for Cluster Builder and Cluster View consists of the network map—the switches, links, and other devices in the cluster—and the menus and toolbar. The toolbar is a quick way to access features also available from the menu bar.

Toolbar Icons for Cluster Builder and Cluster View

One of the ways you can configure cluster switches is by clicking on a toolbar icon. Figure 2-4 shows the Cluster Builder and Cluster View toolbar icons. Hold the cursor over an icon to display the feature invoked by that icon.

*Figure 2-4   Features Available Through the Toolbar*
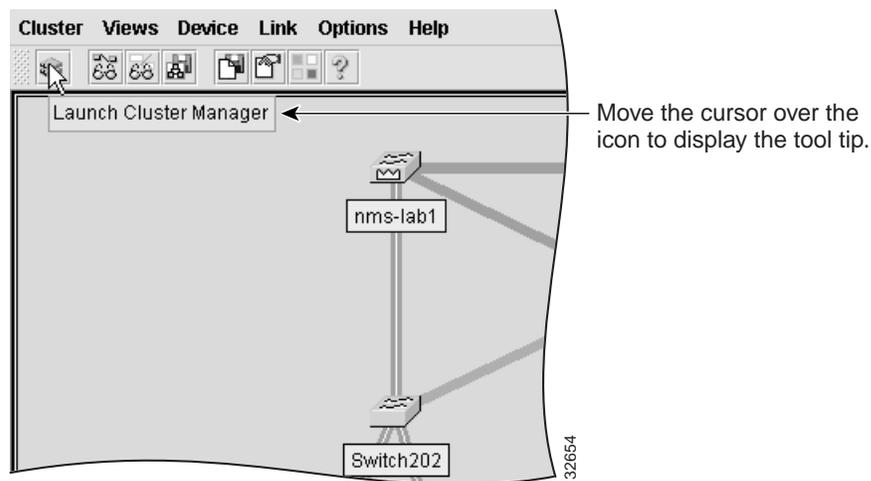
You can invoke the following features from the Cluster Builder or Cluster View toolbar (from left to right):

- Launch Cluster Manager

- Toggle between Cluster Builder and Cluster View

- Toggle between switch names and IP or MAC addresses and connected port numbers.

- Save the presentation of the cluster icons as you have arranged them.

- Save the current configuration for all cluster members to Flash memory.

- Set the user settings for Cluster Builder and Cluster View.

- Display the legend that describes the icons, labels, and links that are used in Cluster Builder and Cluster View.

- List the online help topics for Cluster Builder and Cluster View.

Cluster View and Cluster Builder Device and Link Icons

The Cluster Builder and Cluster View legend shows the meaning of the colored labels and icons that represent the links and devices that make up the cluster. Select **Help>Legend** to display the legend. Figure 2-5 shows the device icons and as they display on the network map. Display the link and label icons by clicking the respective tabs.

Figure 2-5   Icons Used in Cluster Builder and Cluster View

Display the meaning of the label icons.

Display the meaning of the links icons.

Device icons as they appear on Cluster Builder and Cluster View.
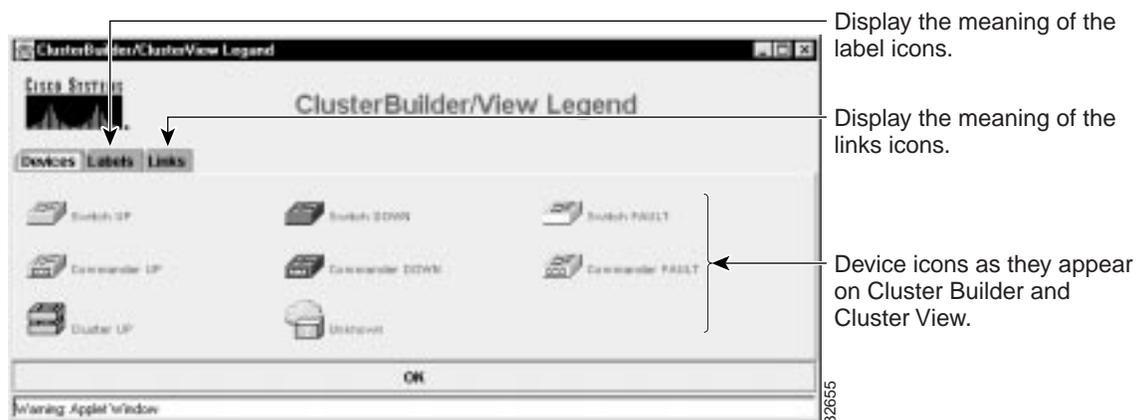
Menu Options for Cluster Builder and Cluster View

Table 2-3 lists the menu options and the tasks you can perform with Cluster Builder and Cluster View.

Table 2-3   Menu Options for Cluster Builder and Cluster View

Menu Bar Choices	Task
Cluster	
Add to cluster	Add candidates to cluster.
Remove from cluster	Remove members from cluster.
User Settings	Change the default settings for the number of hops to discover and the polling interval for Cluster Builder and the link graphs.
Goto Cluster Manager	Start Cluster Manager.
Views	
Toggle Views	Toggle between Cluster Builder and Cluster View.
Toggle Labels	Toggle between switch names and IP or MAC addresses and connected port numbers.
Device	
Launch Switch Manager	Start Switch Manager for a selected switch.
Bandwidth Graph	Display a graph showing the current bandwidth in use by a selected switch. Not supported for Catalyst 1900 and 2820 switches.
Show/Hide Candidates	Expand or collapse image of all candidates connected to a cluster member.
Host Name Configuration	Change the host name for a selected device.
Link	
Link Graph	Display a graph showing the bandwidth being used for the selected link.

Table 2-3   Menu Options for Cluster Builder and Cluster View (continued)

Menu Bar Choices	Task
Link Report	Display the Link Report for two connected devices. If one device is an unknown device, candidate switch, or Catalyst 1900 or 2820 switch, only the cluster member side of the link is displayed.
Options	
Save Layout	Save the current presentation of the network map.
Save Configuration	Save the current configuration of cluster members to Flash memory.
Help	
Contents	List all of the available online help topics.
Legend	Display descriptions of the icons used on the network map.
About	Display the version number for Cluster Builder and Cluster View.

Using Cluster Builder

Follow the procedure in "Accessing CMS for the First Time" section on page 2-8 to display Cluster Builder. When you are using Cluster Manager, click the double-switch icon on the toolbar (Figure 2-4) to toggle back to Cluster Builder.

Use Cluster Builder to create and manage a cluster of switches. Switches connected to the command switch or cluster-capable devices display themselves as cluster members or candidates. Figure 2-6 shows Cluster Builder displaying a map of cluster devices.

Table 2-4 shows the meanings of the label colors in Cluster Builder. Table 2-5 shows the meanings of the link colors in Cluster Builder. Table 2-6 shows the meanings of the icon colors in Cluster Builder.

Table 2-4   Device Label Color Meanings in Cluster Builder

Label Color	Color Meaning
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 with Cluster Builder.
White	A standby command switch.
Yellow	An unknown edge device that cannot become a member.

Table 2-5   Link Color Meanings in Cluster Builder

Link Color	Color Meaning
Dark blue	Active link
Red	Blocked link

Table 2-6   Icon Color Meanings in Cluster Builder

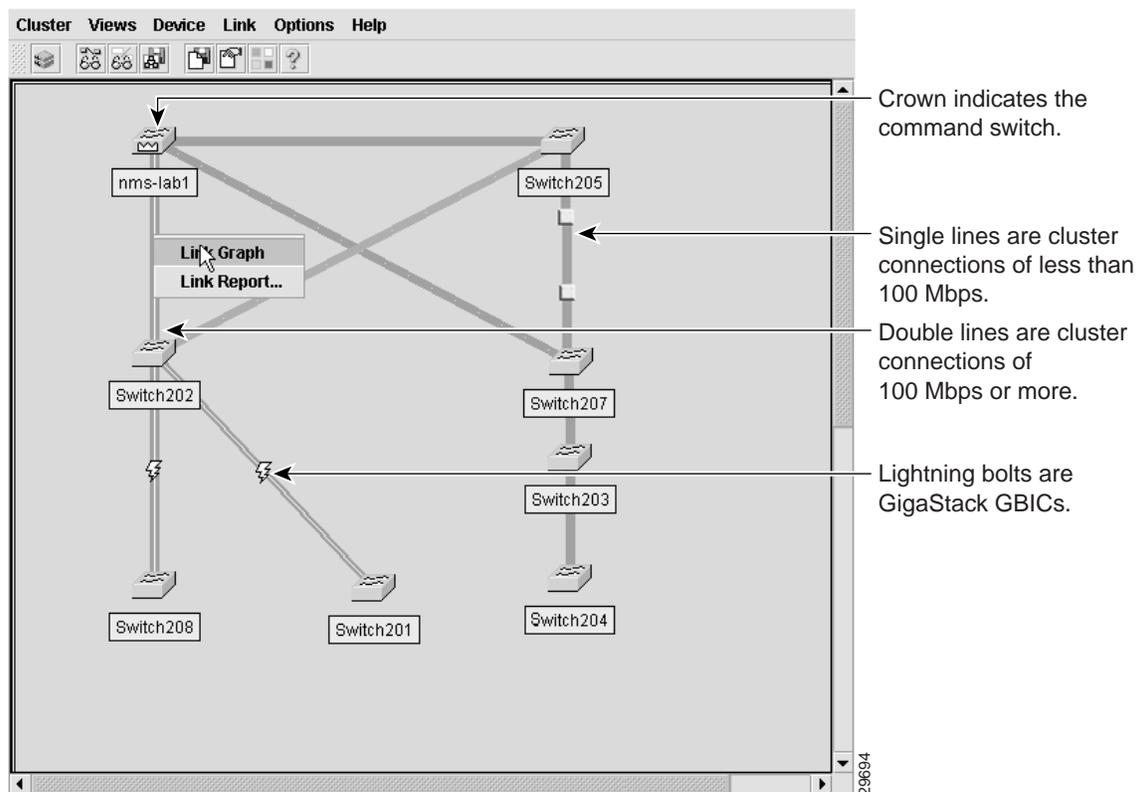| Label Color	Color Meaning
Green	Device is up.
Red	Device is down.
Yellow	Fault Indication.

Figure 2-6   Cluster Builder

Table 2-7 describes the available menu options when you right-click a candidate switch.

Table 2-7   Cluster Builder Candidate Pop-up Menu

Menu Item	Action
Device Web Page	Displays the device-management page for the device.
Add to Cluster	Adds the selected candidate or candidates to the cluster.

Table 2-8 describes the available menu options when you right-click a member switch. For more information on configuring cluster members, see Chapter 4, "Managing Switches."

Table 2-8   Cluster Builder Member Pop-up Menu

Menu Item	Action
Switch Manager	Display the VSM Home page for the selected device.
Bandwidth Graph	Display a graph that plots the total bandwidth used by the switch. This feature is not available on Catalyst 1900 or 2820 switches.
Host Name Config	Change the name of the switch. For more information, see the "Changing the Host Name" section on page 3-31.
Remove from Cluster	Remove the selected switch from the cluster.
Show or hide Candidates	Toggle between displaying candidate switches and not displaying them.
Clear State	Return switches that were down but are now up to the green (up) state. Switches that are yellow are down or were previously down. Applicable only to yellow member switches.

Table 2-9 describes the available menu options when you right-click a link. For more information on displaying link information, see Chapter 6, "Creating Performance Graphs and Link Reports."

Table 2-9   Cluster Builder Link Pop-up Items

Menu Item	Action
Link Graph	Display the performance graph for the link. 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 any mix of Catalyst 1900 and 2820 switches cannot be graphed.
Link Report	Displays information about the two ports in a link between members. If one end of the link is a candidate, the report only displays information about the member switch.

Using Cluster View

Cluster View displays a cluster as a double-switch icon with connections to edge devices and candidate switches. To access Cluster View, select **Views>Toggle Views** from the menu bar in Cluster Builder. Table 2-10 describes the available menu options when you right-click an icon in Cluster View.

Figure 2-7   Cluster View
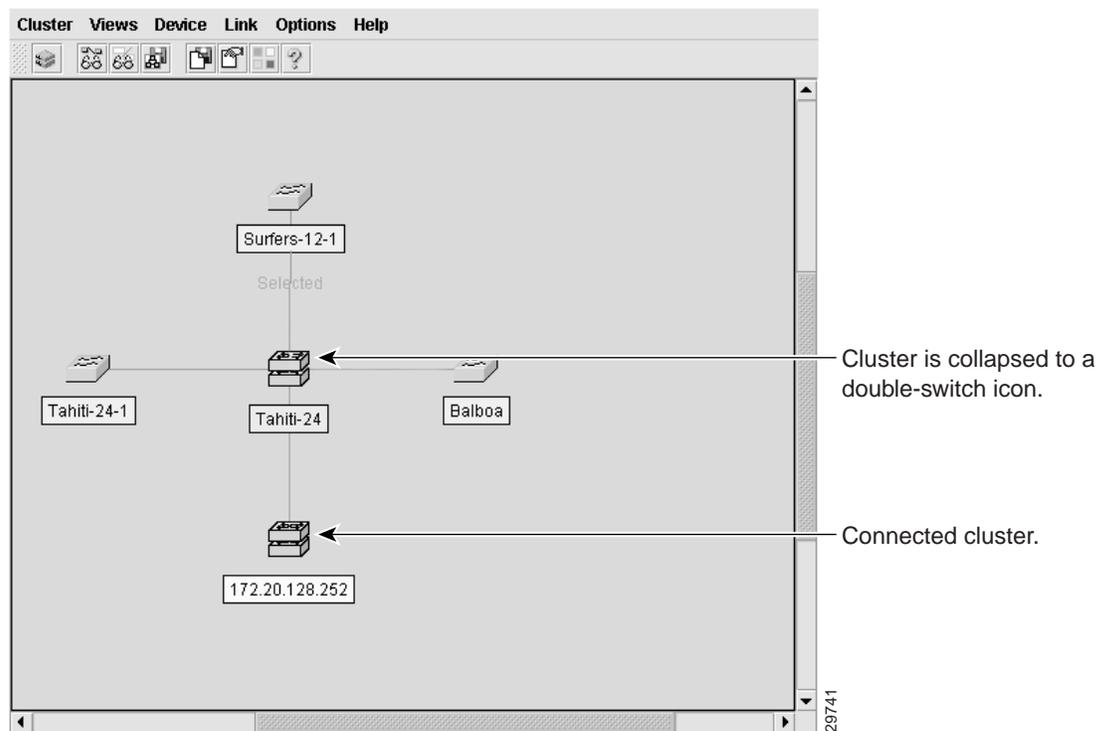
*Table 2-10   Cluster View Device Menu Options*

Menu Item	Action
Device web page	Displays the web management page for the device.
Disqualification code	Describes why the switch is not a cluster member or candidate.

Using Cluster Manager

Follow the procedure in the "Accessing CMS for the First Time" section on page 2-8 to display Cluster Manager. When you are using Cluster Builder, click the double-switch icon on the toolbar (Figure 2-4) to toggle back to 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. With this release, many device-management features that were part of Visual Switch Manager (VSM) are available in Cluster Manager *and* VSM.

Figure 2-8   Cluster Manager
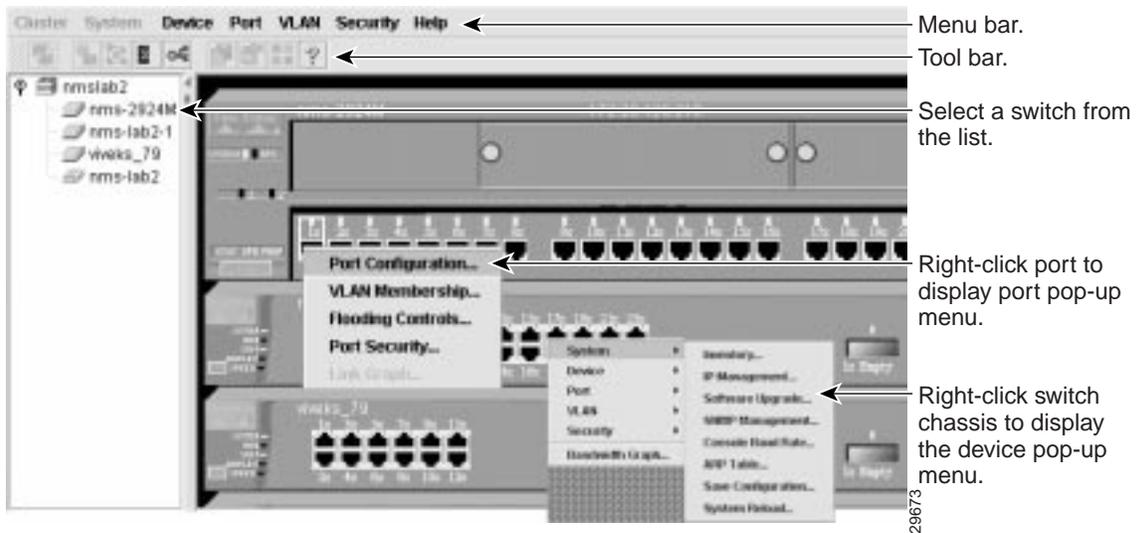
Menu Bar Options in Cluster Manager

Table 2-11 describes the options available from the Cluster Manager menu bar.

Table 2-11   Menu Bar Options Available in Cluster Manager

Menu Item	Task
Cluster	
Management VLAN	Change the management VLAN for a cluster.
System Time Management	Configure the system time or configure the Network Time Protocol.
VMPS Configuration	Configure the VLAN Membership Policy Server.
Standby Command Configuration	Create an HSRP standby group to provide command-switch redundancy.
Device Position	Rearrange the order in which switches appear in Cluster Manager.
User Settings	Set the polling interval for Cluster Manager, Cluster Builder, and the performance graphs. Set the application to display by default.
Cluster Builder	Display Cluster Builder.
System	
Administrative Information	Display the device type, software version, IP address, and other information about a switch or a cluster of switches.
IP Management	Configure IP information for a switch.
Software Upgrade	Upgrade the software for a cluster or a switch.
SNMP Management	Enter SNMP community strings and configure end stations as trap managers.
Console Baud Rate	Change the baud rate of a switch console port.
ARP Table	Display and maintain the Address Resolution Protocol (ARP) table.
Save Configuration	Save the configuration on one or all of the cluster switches.
System Reload	Reboot the software on a switch or a cluster.
Device	
Cisco Group Management Protocol (CGMP)	Enable and disable CGMP and the CGMP Fast Leave feature on a switch.

Table 2-11   Menu Bar Options Available in Cluster Manager (continued)

Menu Item	Task
Spanning-Tree Protocol (STP)	Display and configure STP parameters for a switch.
Port	
Port Configuration	Display and configure port parameters on a switch.
Port Grouping (EC)	Group ports into logical units for high-speed links between switches.
Switch Port Analyzer (SPAN)	Enable SPAN port monitoring.
Flooding Control	Enable storm control and block unicast and multicast flooding on a per-port basis.
VLAN	
VLAN Membership	Display VLAN membership, assign ports to VLANs, and configure Inter-Switch Link (ISL) and IEEE 802.1Q trunks.
VTP Management	Display and configure the VLAN Trunk Protocol (VTP) for interswitch VLAN membership.
Security	
Address Management	Enter dynamic, secure, and static addresses into a switch address table, and define the forwarding behavior of static addresses.
Port Security	Enable port security on a port.
Help	
Contents	List all of the available online help topics.
Legend	Display the legend that describes the icons, labels, and links.
About Cluster Manager	Display the version number for Cluster Manager.

Using the Port Pop-Up Menu to Configure Ports

For port-level configuration, right-click a port to display the port pop-up menu. To configure several ports as a time, press the **Ctrl** key, and right-click ports on the same or different switches. Table 2-12 describes the items available from this menu.

Table 2-12   Cluster Manager Port Pop-up Menu

Menu Item	Action When You Right-Click a Port
Port Configuration	Configure the status, speed, duplex settings and other port-level parameters. For more information, see the "Monitoring and Configuring Ports" section on page 3-37.
VLAN Membership	Define the VLAN mode for a port or ports and add ports to VLANs. Not available for 1900 or 2820 switches.
Flooding Controls	Block the normal flooding of unicast and multicast packets and enable the switch to block packet storms. Not available for 1900 or 2820 switches.
Port Security	Enable port security on a port. Not available for 1900 or 2820 switches.
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 Graphs" section on page 6-1. **Note** This feature is only available when selecting an individual port.

Using the Device Pop-Up Menu to Configure a Switch

For device-level configuration, right-click the switch chassis or a switch in the cluster tree to display the device pop-up menu. The options listed on the pop-up menu are the same as those available in the drop-down menu, with the exception of the Cluster menu. Table 2-13 describes the items available from this menu.

Table 2-13   Cluster Manager Device Pop-up Menu

Menu Bar Choices	Task
System	
Inventory	Displays the device type, software version, IP address, and other information about a switch or cluster of switches.
IP Management	Configure IP information for a switch.
Software Upgrade	Upgrade the software for a cluster or a switch.
SNMP Management	Enter SNMP community strings and configure end stations as trap managers.
Console Baud Rate	Change the baud rate for one or more switches.
ARP Table	Manage the Address Resolution Protocol (ARP) table.
Save Configuration	Save the configuration on one or all of the cluster switches.
System Reload	Reboot the software on a switch or a cluster.
Device	
Cisco Group Management Protocol (CGMP)	Enable and disable CGMP and the CGMP Fast Leave feature on a switch.
Spanning Tree Protocol (STP)	Change STP parameters to prevent network loops.
Port	
Port Configuration	Display and configure port parameters on a switch.

Table 2-13   Cluster Manager Device Pop-up Menu (continued)

Menu Bar Choices	Task
Port Grouping (EC)	Group ports into logical units for high-speed links between switches.
Switch Port Analyzer (SPAN)	Enable SPAN port monitoring.
Flooding Control	Enable broadcast storm control and block unicast and multicast flooding on a per-port basis.
VLAN	
VLAN Membership	Display VLAN membership, assign ports to VLANs, and configure ISL and IEEE 802.1Q trunks.
VTP Management	Display and configure the VLAN Trunk Protocol (VTP) for interswitch VLAN membership.
Security	
Address Management	Enter dynamic, secure, and static addresses into a switch address table, and define the forwarding behavior of static addresses.
Port Security	Enable port security on a port.
Bandwidth Graph	Display 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 Link Graphs" section on page 6-1.

Using the Cluster Tree

The cluster tree displays the name of the cluster and the status of cluster members. Left-click a switch icon in the cluster tree to select it, and right-click to display the device pop-up menu.
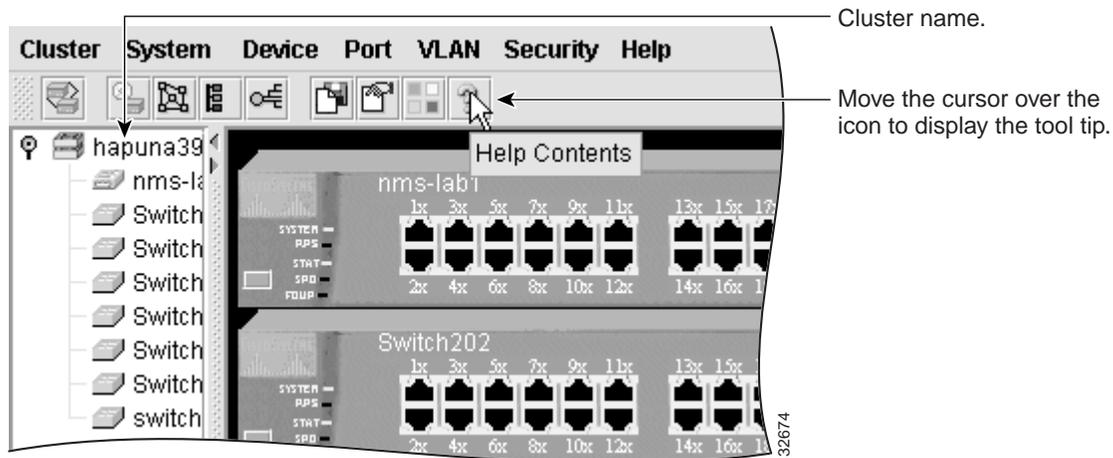
Note   A Catalyst 3524-PWR XL displays as yellow in the cluster tree if it is overheating or if the fan is broken.

Toolbar Icons for Cluster Manager

You can click the toolbar icon to invoke some Cluster Manager features. As shown in Figure 2-9, a description of the icon displays when you move the cursor over it.

Figure 2-9   Cluster Manager Toolbar Icons

Click a Cluster Manager toolbar to invoke the following features, from left to right:

- Start Cluster Builder
- Display the Software Upgrade window
- Display the SNMP Management window
- Display the VLAN Membership window
- Display the Spanning Tree Protocol window
- Display the Save Configuration window
- Display the User Settings window
- Display the legend that describes the icons, labels, and links
- Display the Help table of contents.

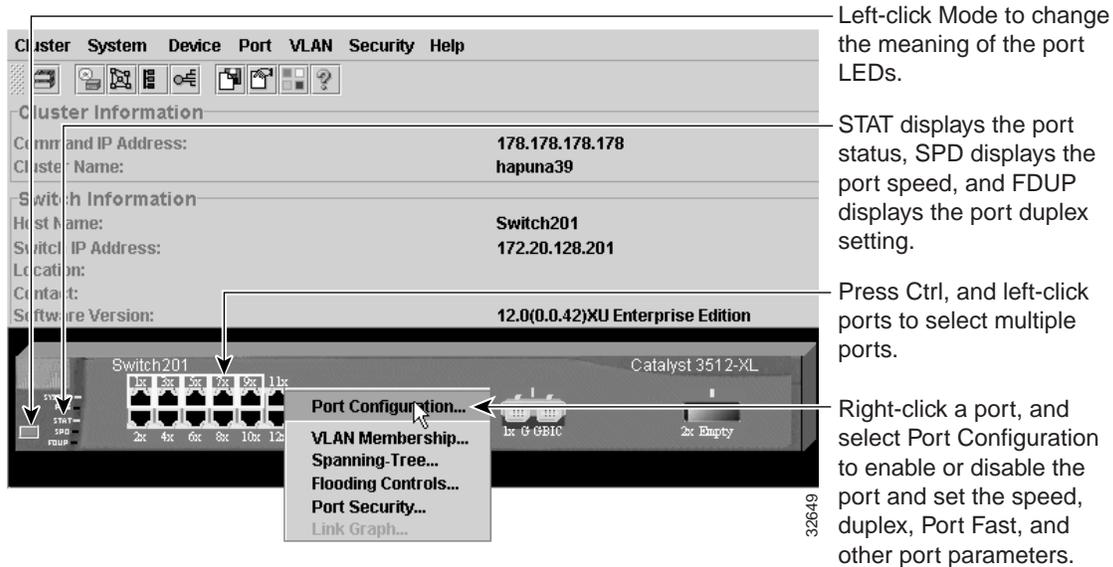**Cisco IOS Desktop Switching Software Configuration Guide**

Using VSM

VSM is a web-based device-management application for configuring and monitoring a clustered or standalone switch. If your switch is part of a cluster, you can also perform many VSM tasks from within Cluster Manager.

If you are using VSM to manage a standalone switch, follow the procedure in "Accessing CMS for the First Time" section on page 2-8 to display the VSM Home page. To display VSM from within Cluster Builder or Cluster View, click on a switch, and select **Device>Launch Switch Manager** from the menu bar.

The VSM Home page displays a real-time image of the switch that you can use to monitor and reconfigure the switch and switch ports. The images of the LEDs displayed by VSM convey the same information as the LEDs on the front panel of the switch. You can configure a port or ports by right-clicking on them and selecting a item from the Port Pop-up menu.

When you use VSM to reconfigure a switch, the change becomes part of the *running configuration* of the switch. The image of the switch and VSM windows always display the switch running configuration. However, the running configuration is not necessarily the startup configuration that is used when the switch restarts. To ensure that your changes are saved after a restart in VSM, select **System>Save Configuration** from the menu bar. If you are using the CLI, you can save the configuration by entering the **write memory** command in privileged EXEC mode.

Figure 2-10   VSM Home Page

Left-click Mode to change the meaning of the port LEDs.

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

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

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

VSM Menu Bar Options

You can access the device-management features from the Home page menu bar. Table 2-14 describes the menu options and their function.

Table 2-14   Menu Bar Options Available in VSM

Menu Bar Choices	Task
Cluster	
Cluster Command Configuration	Enable a switch to act as the cluster command switch.
Cluster Management	Display Cluster Manager or Cluster Builder.
System	
Inventory	Display the device type, software version, IP address, and other information about a switch.
IP Management	Configure IP information for a switch.

Table 2-14   Menu Bar Options Available in VSM (continued)

Menu Bar Choices	Task
Software Upgrade	Upgrade the software for the cluster or a switch.
System Time Management	Configure the system time or the Network Time Protocol (NTP).
SNMP Management	Enter SNMP community strings and configure end stations as trap managers.
Console Baud Rate	Change the baud rate for a switch.
ARP Table	Display the device Address Resolution Protocol (ARP) table.
User Settings	Change the polling intervals for clustering and graphing, and enable the display of the splash page when VSM starts.
Save Configuration	Save the configuration.
System Reload	Reboot the software on a switch.
Device	
Cisco Group Management Protocol (CGMP)	Enable and disable CGMP and the CGMP Fast Leave feature on a switch.
Spanning-Tree Protocol (STP)	Display and configure STP parameters for a switch.
Port	
Port Configuration	Display and configure port parameters on a switch.
Port Grouping (EC)	Group ports into logical units for high-speed links between switches.
Switch Port Analyzer (SPAN)	Enable SPAN port monitoring.
Flooding Control	Enable broadcast storm control and block unicast and multicast flooding on a per-port basis.
VLAN	
VLAN Membership	Display VLAN membership, assign ports to VLANs, and configure ISL and 802.1Q trunks.
Management VLAN	Change the management VLAN on the switch.

Table 2-14   Menu Bar Options Available in VSM (continued)

Menu Bar Choices	Task
VTP Management	Display and configure the VLAN Trunk Protocol (VTP) for interswitch VLAN membership.
VMPS Configuration	Configure the VLAN Membership Policy Server
Security	
Address Management	Enter dynamic, secure, and static addresses into a switch address table. You can also define the forwarding behavior of static addresses.
Port Security	Enable port security on a port.
Help	
Contents	List all of the available online help topics.
Legend	Display the legend that describes the icons, labels, and links.
About Visual Switch Manager	Display the version number for Visual Switch Manager.

VSM Port Pop-Up Menu and Device Pop-Up Menu Options

The options available through the port pop-up and device pop-up menus in VSM are the same as those described in Table 2-12 and Table 2-13.

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 Certain port features can conflict with one another. Review the "Managing Configuration Conflicts" section on page 4-2 before you change the port settings.

Understanding the CLI

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

The switch supports the following command modes:

- User EXEC
- Privileged EXEC
- VLAN database
- 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.
VLAN database	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.

Table 2-15   Command Modes Summary (continued)

Modes	Access Method	Prompt	Exit Method	About This Mode[1]
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**. To exist to privileged EXEC mode, enter **Ctrl-Z** or **end**.	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**. To exist to privileged EXEC mode, enter **Ctrl-Z** or **end**.	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 7-3.

When the Cluster Builder 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 for the Cluster Management Suite, see the "Changes to Passwords" section on page 3-11.

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 VSM and the Cluster Management Suite. You must also use privilege level 15 if you configure the TACACS+ (Terminal Access Controller Access Control System Plus) protocol from 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 from 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 2-39.

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* creates 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 space and a 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 space and a question mark (?). The possible keywords that you can enter with the command are displayed.
`% 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

Follow these steps to configure a Telnet password:

	Command	Purpose
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	**enable**	Enter privileged EXEC mode.
Step 3	**config terminal**	Enter global configuration mode.
Step 4	**line vty 0 15**	Enter the interface configuration mode for the Telnet interface.
		There are 16 possible sessions on a command-capable switch. The 0 and 15 mean that you are configuring all 16 possible Telnet sessions.
Step 5	**password** *<password>*	Enter a password.
Step 6	**end**	Return to privileged EXEC mode so that you can verify the entry.
Step 7	**show running-config**	Display the running configuration.
		The password is listed under the command **line vty 0 15**
Step 8	**copy running-config startup-config**	(Optional) Save the running configuration to the startup configuration.

The "Finding More Information About IOS Commands" section on page 4-1 contains the path to the complete IOS documentation.

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. This could be useful if you wanted to save configuration files on an external server in case a switch fails. You can then copy the configuration file back to a replacement switch and avoid having to reconfigure the switch.

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 config.text from the host *arno* to the switch Flash memory:

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

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

- TFTP
- Flash
- RCP
- XMODEM

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 Simple Network Management Protocol (SNMP) to access the MIB variables
- Managing cluster switches through SNMP

Note   When configuring your switch by using SNMP, note that certain combinations of port features create configuration conflicts. For more information, see the "Managing Configuration Conflicts" section on page 4-2.

CiscoWorks2000 and CiscoView 5.0 are network-management applications you can use to configure, monitor, and troubleshoot 2900 and 3500 XL switches.

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.

You can also access this server from your browser by entering the following URL in the **Location** field of your Netscape browser (the **Address** field in Internet Explorer):

`ftp://ftp.cisco.com`

Use the mouse to navigate to the folders listed above.

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 that can be compiled with your network management software

An example of an NMS is the CiscoWorks network management software. CiscoWorks2000 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 2-11, 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 2-11   SNMP Network
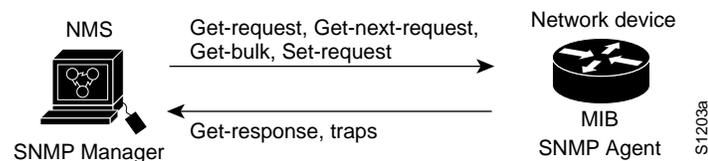
Table 2-17   SNMP Operations

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 Cluster Switches 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 4-34. 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.

Note   When the a standby group is configured, the command switch can change without the user's knowledge. Use the first read-write and read-only community strings to communicate with the command switch if there is a standby group configured for the cluster.

If the member switch does not have an IP address, the command switch passes traps from the member switch to the management station, as shown in Figure 2-12. 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 3-10 and the "Configuring SNMP" section on page 4-34.

Figure 2-12   SNMP Management for a Cluster
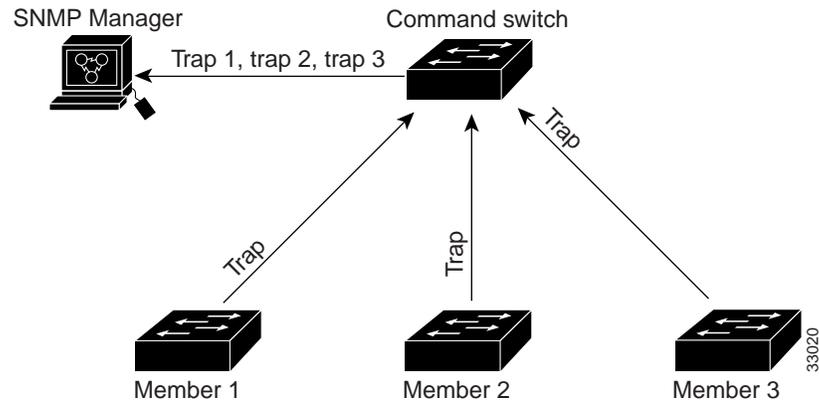
RMON Support

This IOS software release supports four Remote Monitoring (RMON 1) groups. You can configure these groups by using an SNMP application or by using the CLI. The four supported groups are alarms, events, history, and statistics.