

Managing Clusters of Switches

A cluster is a group of connected switches that are managed as a single entity. The switches can be in the same location, or they can be distributed across a network. All communication with cluster switches is through one IP address. You can have up to 16 switches in a cluster: 1 *command* switch and 15 *member* switches.

This chapter describes how to create and manage clusters of switches by using Cluster Management. Cluster Management has three components:

- Cluster Builder
- Cluster Manager
- Cluster View

Cluster Management interface and navigation techniques are described in Chapter 2, “Using the Management Interfaces.”

Command and Member Switches

The *command* switch is the single point of access used to configure and monitor the switches in a cluster. A *member switch* is managed through a command switch. Command switches must be running a version of IOS Release 11.2(8)SA6 software that supports the ability to be a command switch. See the “Supported Hardware” section on page 1-2 for the complete list of command-capable switches.

When you first install your switches, you cable the switches together and assign an IP address to the command switch. In addition, you must enable the switch as the command switch. When the switches are turned on, the command switch uses information from Cisco Discovery Protocol (CDP) to identify *candidate* switches that you can add to a cluster. After the cluster is formed, you can access all switches in the cluster by entering the IP address

of the command switch. The password you enter when you log in to the command switch also gives you access to cluster member switches. If the command switch fails, you can use its password to create a new command switch for the cluster.

Note Links between a command switch and cluster member and candidate switches must be through ports that belong to VLAN 1.

Creating Clusters

After you have assigned an IP address to a switch and connected it to other switches running IOS Release 11.2(8)SA6, you can use Cluster Builder to create a cluster with one IP address. The switch assigned the IP address must be command-capable for it to be the command switch, and you must explicitly enable it to be the command switch on the CVSM home page. Command-capable switches that are not cluster members have two additional fields that appear on the switch home page: the **Command Switch** and the **Cluster Name** field. Use these fields to enable a switch as the command switch and enter the cluster name.

Cluster Builder displays by default when you click **Cluster Management** from a CVSM home page or the Cisco Access page. You can use Cluster Builder to access the following features:

- Display the CVSM home page for a cluster switch
- Toggle between the IP addresses (or MAC addresses) of cluster switches and the names of cluster switches
- Display the device links between the command switch and member switches
- Display link reports and graphs, and device-reports and graphs
- Save all cluster member configurations to permanent storage
- Display the User Settings dialog box to change the default view and set the polling times for Cluster Builder and the device and link graphs
- Display Cluster Manager
- Toggle between Cluster Builder and Cluster View

Planning Your Cluster

How you create a cluster depends on your network. If the switches are arrayed in a star topology with the command switch at the center, you can add all the switches to the cluster at once. If the switches are connected in a daisy-chain topology, you add the candidate connected to the command switch and then continue adding each switch in the chain as it is discovered by CDP. If switches are daisy-chained off of a star topology, you can add all the switches directly connected to the command switch and then add the daisy-chained switches one at a time.

There can be a maximum of 16 switches in a cluster: 15 member switches and 1 command switch. If there are passwords defined for the candidate switches, you must know them before they can be added to the cluster. In addition, a candidate switch must satisfy the following requirements to join a cluster:

- It is running IOS Release 11.2(8)SA6 or later.
- It has CDP enabled.
- It is connected to a command switch through ports that belong to VLAN 1.
- It is connected to a command switch through ports that are in an STP forwarding state.
- It is not a member switch or a command switch of another active cluster.

If a switch does not become part of the cluster, right-click it and select **Disqualification Code** to display the reason it did not join the cluster.

Configuring a Backup Command Switch

If the command switch fails, member switches continue forwarding but cannot be managed through the command switch. Member switches retain the ability to be managed through normal standalone means, such as the console-port CLI, and they can be managed through SNMP, HTML, and Telnet after they have been assigned an IP address.

You can recover from a failed command switch by replacing the failed unit with a cluster member or another switch. To have a cluster member ready to replace the command switch, assign an IP address to a cluster member, and know the command-switch enable password. To use Telnet, you also need to know the login password. The cluster member must be running software that allows it to become a command switch. See “Supported Hardware” section on page 1-2 for the list of switches that can be command switches.

Redundant links from the backup command switch to the cluster make for a faster replacement in the event of failure but are dependent on your topology. For the actual recovery procedures, see the “Recovering from a Command Switch Failure” section on page 5-7.

Automatically Discovering Cluster Candidates

Cluster Builder automatically prompts you to add cluster members when it first starts and when the topology changes. When Cluster Builder starts, a dialog box lists the candidate switches with their device types, MAC addresses, and the ports through which they are directly connected to the command switch. Only switches that are directly connected to the command switch can be added in this way.

You can set Cluster Builder to not automatically display suggested candidates. See the “Changing User Settings” section on page 4-10 for instructions.

Figure 4-1 shows the dialog box for adding switches to a cluster. When the command switch presents the list of candidates, you can accept the suggested cluster or not. If you do not accept the suggested cluster, none of the switches are added, and members must be added one at a time. If you accept the cluster and there are more switches daisy-chained to a cluster member, they must be added one at a time.

You are prompted to enter a password at this point. Enter the enable password of the candidate switch if one has been defined. If no password has been defined for the candidate, click **OK** to add it to the cluster with no password.

If you enter a password that does not match the password defined for the candidate, or if you enter a password for a candidate that has not had a password defined for it, the switch is not added to the cluster. In all cases, once a candidate switch joins a cluster, it takes the enable password of the cluster command switch.

For more information on entering switch passwords, see the “Setting Passwords” section on page 2-26.

Note The cluster configuration is saved only when you click **Save Configuration** on the command switch. This saves the configuration on the command switch and on the member switches.

Figure 4-1 Adding Switches to a Cluster

Do you want to add these candidate devices to the cluster?
Selected devices have been pre-qualified by the command switch

Name	Device Type	MAC Address	Upstream Switch
tahiti-112	cisco VWS-C3512	0050.5494.2b40	switch201

Enable password for candidate devices:

OK to add all selected candidates to the cluster.
Cancel to continue without adding.

Show suggested candidates everytime Cluster Builder starts

24327

Enter the password of the candidate switch. If no password exists for the switch, leave this field blank for the switch to join the cluster.

When the Cluster Is Created

When a cluster is formed, the command switch automatically changes three parameters on the cluster member switches: the IOS host name, the enable password, and the SNMP community string.

If a switch has not been assigned an IOS host name, the command switch appends a number to the name of the command switch and assigns it sequentially to the member switches. For example, a command switch named *eng-cluster* could name a cluster member *eng-cluster-5*. If an IOS host name has already been assigned to a switch, it retains the name.

For the SNMP community strings, the command switch adds the following SNMP community strings to a member switch when it is added to a cluster:

- commander-readonly-community-string
- commander-readonly-community-string@esN, where N is the member switch number.
- commander-readwrite-community-string
- commander-readwrite-community-string@esN, where N is the member switch number.

For the enable password, the command switch configures the member switch with its password when the switch joins the cluster.

CLI Commands for Creating a Cluster

The same requirements for creating a cluster apply when you use the CLI to create it. Follow these steps to enable the cluster command switch and add member switches to a cluster:

Step 1 Enable the cluster commander:

```
switch> enable
Password: <password>
switch#
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# cluster enable An-Example-Cluster
switch(config)# exit
switch#
```

Step 2 Now discover the candidates:

```
switch# show cluster candidates

00E0.1E00.2222 Switch cisco WS-C2924-XL Fa0/16 1 0 Fa0/1
00E0.1E00.3333 Switch cisco WS-C2924-XL Fa0/1 1 0 Fa0/2
```

Step 3 Configure both candidates as cluster members:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# cluster member 2 mac-address 00E0.1E00.2222
switch(config)# cluster member 4 mac-address 00E0.1E00.3333
switch(config)# exit
```

Step 4 Display status of the cluster:

```
switch# show cluster members
```

MN	Mac Address	Link Interface	Hops	Upstream SN	Upstream Interface	State
2	00E0.1E00.2222	Fa0/16	1	0	Fa0/1	Up
4	00E0.1E00.3333	Fa0/1	1	0	Fa0/2	Up

Adding and Removing Cluster Members

You can use the network map to add switches to the cluster (see Figure 4-2). Switches in the cluster are green, candidates are blue, and other connected devices that are running CDP are yellow. Follow these steps to add a switch to a cluster:

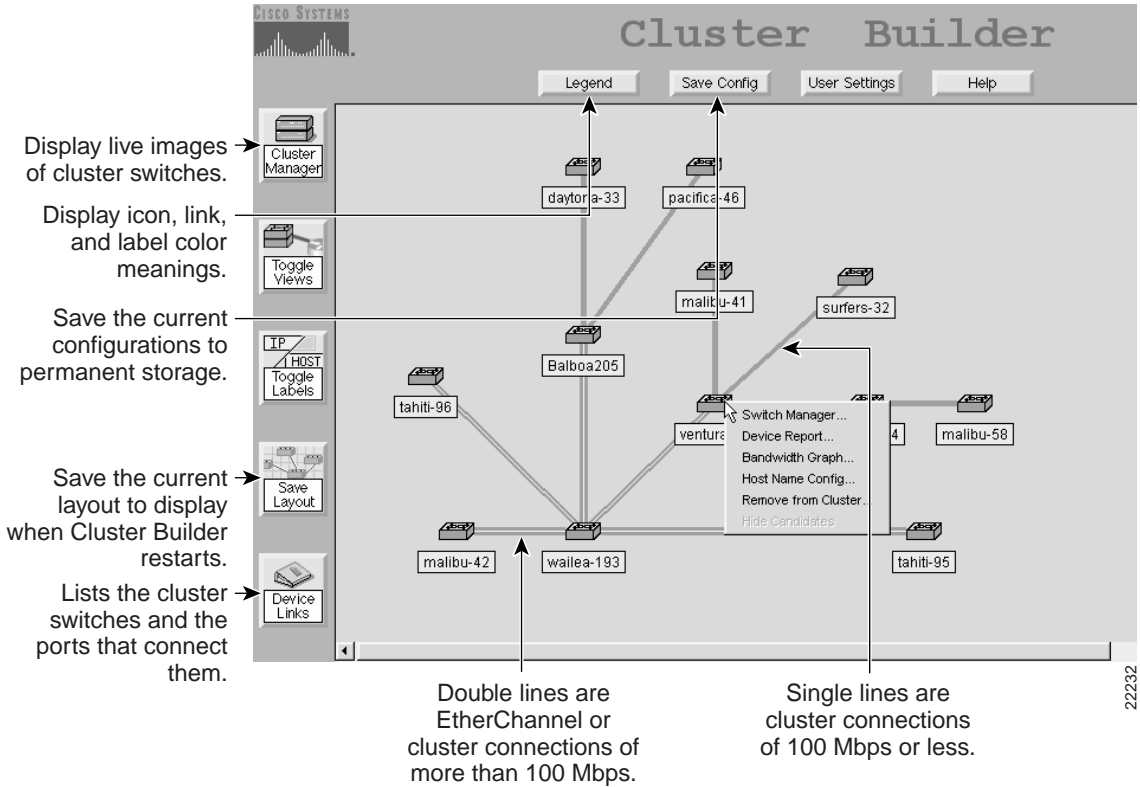
Step 1 Right-click a candidate (blue) switch to display the pop-up menu.

Step 2 From the pop-up menu, select **Add to Cluster**.

To remove a device, right-click a member switch, and select **Remove from Cluster** on the pop-up menu.

To hide or display candidate switches, click either **Hide Candidates** or **Show Candidates**.

Figure 4-2 Cluster Builder



CLI Commands for Removing a Cluster Member

Follow these steps to remove a member switch from a cluster:

- Step 1** Display the status of the cluster and note the MAC address of the switch you want to remove:

```
switch# show cluster members
```

```

|---Upstream---|
SN MAC Address      Name           PortIf  FEC Hops  SN PortIf  FEC  State
0  0050.5494.3c40  Tahiti-24          0      0
2  00e0.1e9f.8c00  Tahiti-24-2   Fa0/4    1      0  Fa0/7    Up

```

- Step 2** Enter global configuration mode:

```
switch# config terminal
```

- Step 3** Remove the switch from the cluster:

```
switch(config)# no cluster member 2 mac-address 00e0.1e9f.8c00
```

- Step 4** Return to privileged EXEC mode:

```
switch# end
```

- Step 5** Display the status of the new cluster:

```
switch# show cluster members
```

```

|---Upstream---|
SN MAC Address      Name           PortIf  FEC Hops  SN PortIf  FEC  State
0  0050.5494.3c40  Tahiti-24          0      0

```

Changing User Settings

Click **User Settings** at the top of the page to change the parameters described in the following list. The user settings are saved in permanent storage on the command switch.

- Cluster Builder and Cluster Manager polling interval—Select the number of seconds the switch waits before polling the switch for new cluster and port information. Lowering the polling interval can be useful when you are changing or testing the cluster switches. The default is 120 seconds.

You must reload (Netscape) or refresh (Internet Explorer) the page when you change this parameter for the new setting to take effect.

- Link and device graph polling interval—Select the number of seconds the switch waits before polling the switch for new graph information. The default is 24 seconds.

You must reload (Netscape) or refresh (Internet Explorer) the page when you change this parameter for the new setting to take effect.

- Show suggested candidate window every time Cluster Management starts: set the switch to prompt the user with new candidates every time Cluster Builder or Cluster Manager is started. Cluster Builder still redraws the map of the network if new devices are discovered.

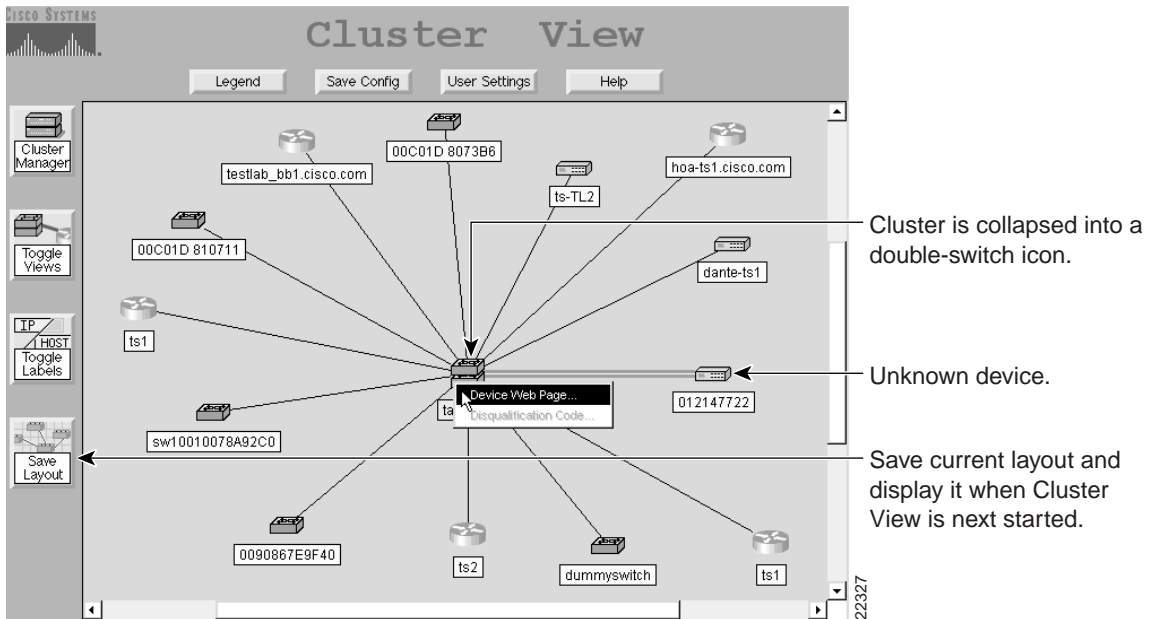
A conflict arises if you set the switch to always discover new candidates and you also have Cluster Manager set to display by default. In this case, you are prompted to display Cluster Builder to add or remove devices from the cluster.

- Change the default view: select Cluster Manager to display it by default when Cluster Management starts.

Displaying Cluster View

From Cluster Builder, click **Toggle Views** to display a map of the cluster and attached devices. In Cluster View, the cluster is condensed into an icon. You can save the view in Cluster View and toggle back and forth to Cluster Builder.

Figure 4-3 Cluster View



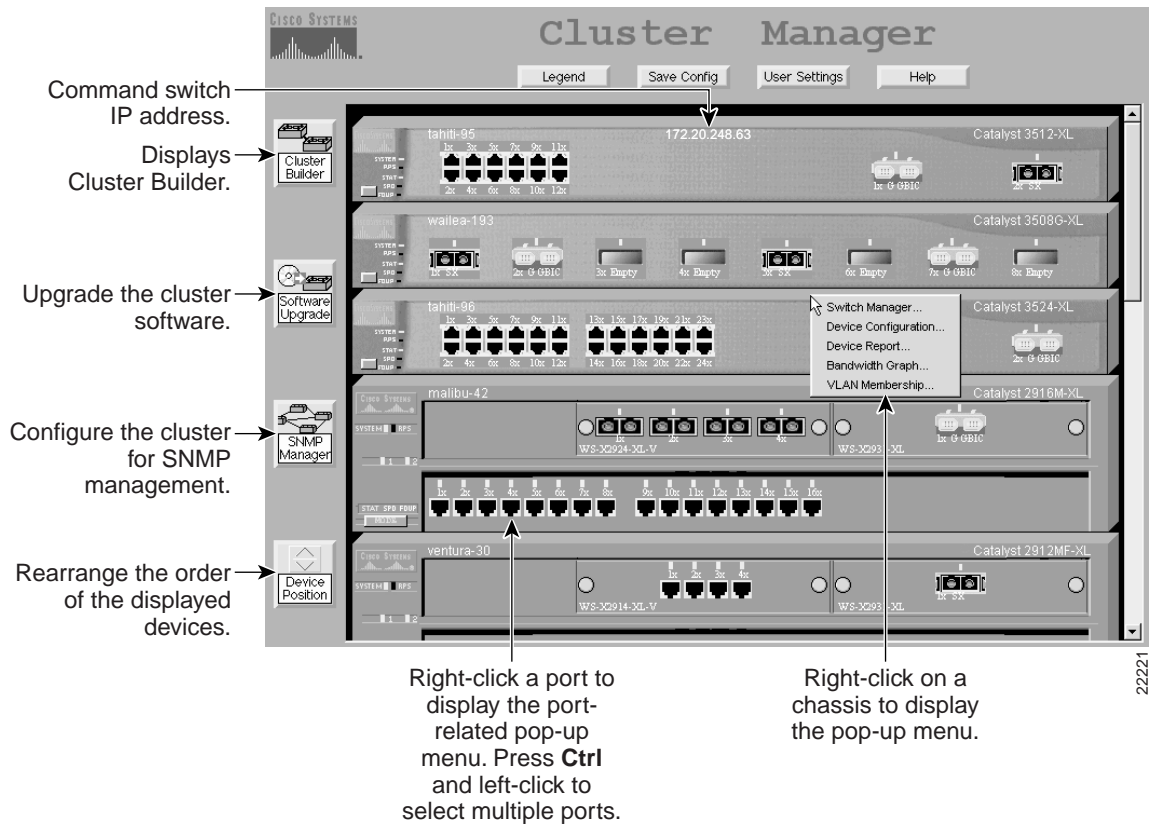
Managing Clusters

After you have created a cluster, you can use Cluster Manager to monitor and configure the switches in the cluster. Figure 4-4 shows a cluster displayed on the Cluster Manager page. The switch software updates the LEDs displayed on these images in real time, making the images displayed by Cluster Manager as informative as the switches themselves. From this page you can perform the following tasks:

- Monitor and configure ports
- Display VLAN information
- Display the CVSM home page for a cluster switch
- Upgrade the switch software for all switches in a cluster

- Enable and configure SNMP for all switches in the cluster
- Rearrange the physical images of the switches
- Display Cluster View
- Display performance graphs
- Display device reports

Figure 4-4 Cluster Manager



Monitoring Port Status

The LEDs above the ports in Figure 4-4 can display the status, speed, or duplex setting of the port. Click the Mode button on the image to highlight in turn each of the settings. STAT displays the link status of the port, SPD displays the speed of the port, and FDUP displays whether the port is operating in half- or full-duplex mode. Click **Legend** to display the meanings of the colors.

Configuring Ports

You can operate on single and multiple ports by clicking them in the Cluster Manager window. The defaults of the different port types and port-configuration guidelines are described in the “Configuring Port Parameters” section on page 3-19.

When you select a port or ports, you can set the following parameters:

- | | |
|-----------|---|
| Status: | Enable or disable the port. |
| Duplex: | Set a port to full-duplex (Full), half-duplex (Half), or autonegotiate (Auto). The default is Auto . For ATM ports, this field is read-only and displays Full . |
| Speed: | Set a 10/100 port to 10 Mbps (10), 100 Mbps (100), or autonegotiate (Auto). The default is Auto .

For Gigabit Ethernet ports, the field displays 1000 and is read-only. For ATM ports, the field displays 155 (155 Mbps) and is read-only. |
| Port Fast | Set the port to come immediately into the STP forwarding state and bypass the normal transition from the listening and learning states to the forwarding state. |

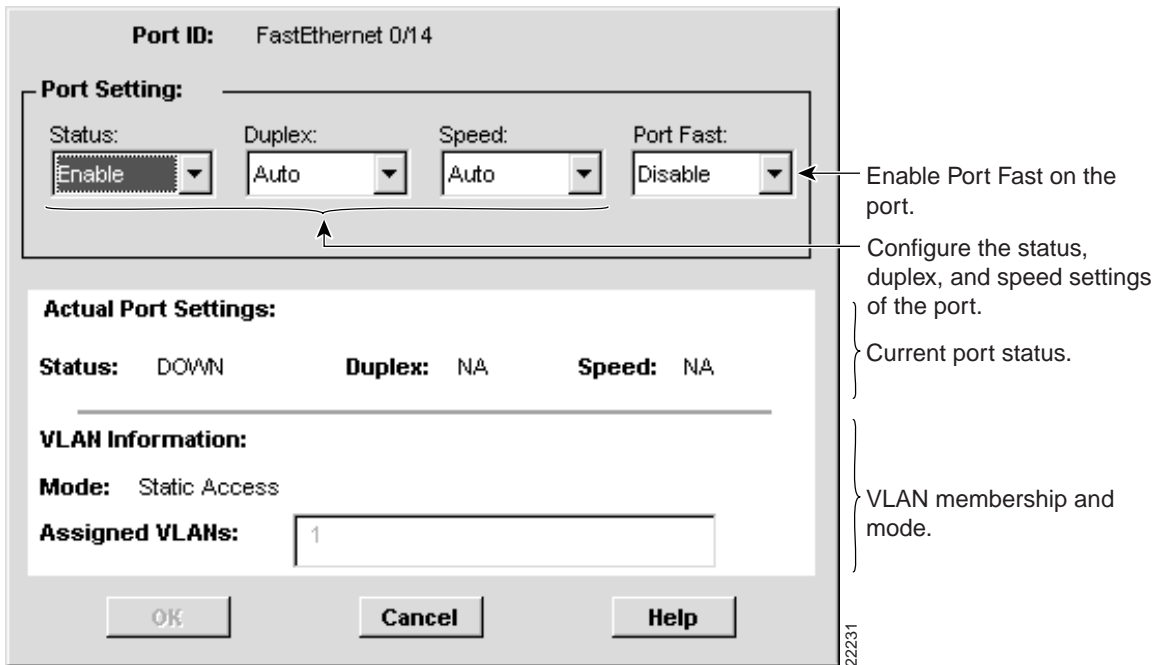
Note The autonegotiation feature can sometimes cause unpredictable results. See the “Connecting To Devices That Do Not Autonegotiate” section on page 3-19, or click **Help** for more information on autonegotiation mismatches.

Configuring a Single Port

Left-click a port to select it, and then right-click to display the pop-up menu. Select **Port Configuration** to display the dialog box shown in shown in Figure 4-5. Use this dialog box to enable or disable the port, change the speed and duplex settings, and enable or disable the STP Port Fast parameter.

When you configure a single port, the dialog box displays the current status and the current settings of the port, the VLAN mode of the port, and the VLANs that the port belongs to.

Figure 4-5 Single Port Configuration

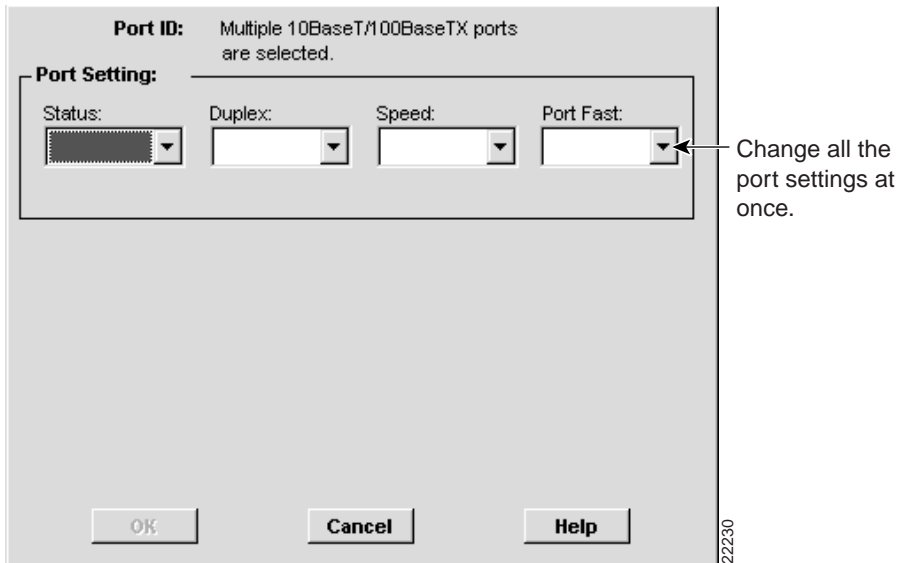


Configuring Multiple Ports

Left-click ports while holding down the **Ctrl** key to select more than one port at a time. After selecting the ports, right-click to display the pop-up menu, and select **Port Configuration**. The window shown in Figure 4-6 displays. You can use this window to change the ports settings for the selected ports, but the window does not display the actual port settings or VLAN information.

For more information on configuring ports, see the “Configuring Port Parameters” section on page 3-19 or click **Help**.

Figure 4-6 Multiple Port Configuration



Displaying VLAN Membership

The VLAN Membership page shown in Figure 4-7 displays the list of all the user-defined VLANs on the switch. By selecting a VLAN, you can display the ports that belong to the VLAN. In addition, the color coding indicates which VLAN mode a port is in.

To display the VLANs that are active on a switch, right-click the chassis of the switch in Cluster Manager. Select **VLAN Membership** from the pop-up menu.

To display the ports that belong to a given VLAN, select the VLAN ID on the VLAN Membership page, and click **Display Members**. Cluster Manager highlights all the ports in the window that belong to the selected VLAN. The Legend on the VLAN Management page shows the colors Cluster Builder uses to indicate the VLAN modes of the ports.

To display the VLAN membership for a single port, right-click the port, and select **Port Configuration** from the pop-up menu.

Figure 4-7 VLAN Membership

VLAN ID	VLAN Name	Status
1	default	active
2	VLAN0002	active
3	VLAN0003	active
4	VLAN0004	active
5	VLAN0005	active
6	VLAN0006	active
7	VLAN0007	active
8	VLAN0008	active
9	VLAN0009	active
10	VLAN0010	active
11	VLAN0011	active
56	VLAN0056	active

Display Members ← Select a VLAN and click Display Members to show the ports in that VLAN.

Legend:

- Static
- Dynamic
- ISL Trunk
- Multi-VLAN
- 802.1Q Trunk
- ATM Trunk

Ports in Cluster Manager are highlighted in these colors when you select a switch and click Display Members.

24328

Upgrading Software for a Group of Switches

You can upgrade cluster switches by using the Software Upgrade window shown in Figure 4-8. New IOS software releases with new features are posted on Cisco Connection Online (CCO) and are available through authorized resellers. You can also download the Cisco TFTP server from CCO.

You can upgrade all or some of the switches in a cluster at once, but the switch performs a series of checks before the upgrade takes place. Organize your upgrades so that the following rules do not slow down the upgrade process:

- Switches from different product lines, such as the Catalyst 2900 series XL and the Catalyst 3500 series XL, cannot be upgraded at the same time.

- Older switches with 4 MB of DRAM cannot be upgraded to an 8-MB image. The 4-MB models are WS-C2908-XL, WS-C2916M-XL, WS-C2924C-XL, and WS-C2924-XL.
- Newer switches with 8 MB of DRAM cannot be upgraded to a 4-MB image.

New images are copied to Flash memory and do not affect the operation of the switch. The switch checks Flash memory to ensure there is sufficient space before the upgrade takes place. If there is not enough space in Flash memory for the new and old image, the new image replaces the old one. If there is enough space, the new image is copied to the switch without replacing the old image, and the old image is deleted after the download of the new image is complete. In this way, you can still restart the switch if the download of the new image fails.

Figure 4-8 Cluster Software Upgrade

The screenshot shows a 'Cluster Software Upgrade' dialog box. At the top, there is a 'TFTP Server IP Address' field containing '172.20.128.202' and a 'New IOS Image File Name' field. Below these is a checkbox labeled 'Retain Current IOS Image file name(s)'. The main area is divided into two lists: 'Available Cluster Members' and 'Selected Cluster Members'. The 'Available' list contains several Catalyst models like 'Catalyst 2916M-XL (malj)', 'Catalyst 2912MF-XL (ver', 'Catalyst 2924M-XL (Ball', 'Catalyst 2916M-XL (malj', 'Catalyst 2924-XL (pacif', 'Catalyst 2924M-XL (ball', 'Catalyst 2916M-XL (malj', and 'Catalyst 2924C-XL (surf'. The 'Selected' list contains 'Catalyst 3512-XL (tahiti-', 'Catalyst 3524-XL (tahiti-', and 'Catalyst 3508G-XL (wailea'. Between the lists are 'Add >>' and '<< Remove' buttons. At the bottom, there is a 'Software Upgrade Status Messages' area, a 'Reboot Cluster' button, and 'Upgrade', 'Cancel', and 'Help' buttons.

Annotations on the left side:

- Files are renamed unless you click here. (points to the 'Retain Current IOS Image file name(s)' checkbox)
- Shows the cluster members that can be upgraded. (points to the 'Available Cluster Members' list)
- Click to restart all the switches that were upgraded. (points to the 'Reboot Cluster' button)

Annotations on the right side:

- IP address of device where the new file is in the TFTP root directory. (points to the 'TFTP Server IP Address' field)
- Upgrade file. (points to the 'New IOS Image File Name' field)
- Shows the cluster members to be upgraded. 3500 XL and 2900 XL switches must be upgraded separately. (points to the 'Selected Cluster Members' list)
- Shows upgrade status and which switches failed to upgrade successfully. (points to the 'Software Upgrade Status Messages' area)

22227

You upgrade the cluster by using a tar file that contains the switch software image and the HTML files for the HTML interface. You can enter just the name of the file or a path. You do not need to enter a path if the image file is in the root directory of the TFTP server.

New features provided by the software are not available until you reload the software.

Configuring the Cisco TFTP Server to Upgrade Multiple Switches

The Cisco TFTP server application can handle multiple requests and sessions, but you must first disable the **Show File Transfer Progress** and the **Enable Logging** options to avoid TFTP server failures. If you are performing multiple-switch upgrades with a different TFTP server, it must be capable of managing multiple requests and sessions at the same time.

CLI Commands for Upgrading Member Switches

As member switches might not be assigned an IP address, command-line software upgrades via TFTP are managed through the command switch. Follow these steps to upgrade the switch software on a member switch:

Step 1 Starting from the command switch in EXEC mode, log in to the member switch:

```
switch# rcommand 1
```

Step 2 Start the TFTP copy as if you were initiating it from the command switch. Press Enter when prompted by the switch:

```
switch1# tar /x tftp://server_ip_address//path/filename.tar flash:
Source IP address or hostname [server_ip_address]?
Source filename [path/filename]?
Destination filename [flash:new_image]?
Loading /path/filename.bin from server_ip_address (via!)
[OK - 843975 bytes]
```

Step 3 Reload the new software with the following command:

```
switch# reload
System configuration has been modified. Save? [yes/no]:y
Proceed with reload? [confirm]
```

You lose contact with the switch while it reloads the software. See the “Understanding the CLI” section on page 2-24 for more information on the **rcommand**.

Configuring SNMP

The command switch manages SNMP communication for all switches in the cluster. The command switch forwards the set and get requests from SNMP applications to member switches, and it forwards the traps and other responses coming from the member switches to the appropriate management station. The description of SNMP configuration in the “Configuring SNMP” section on page 3-43 also applies to the use of the page shown in Figure 4-9.

Configuring Community Strings

Use the SNMP Manager page (Figure 4-9) to enter read-write and read-only community strings for an entire cluster. Community strings provide authentication in the exchange of SNMP messages. The command switch appends numbers to the community strings of member switches so that these modified community strings can provide authentication for the member switches. When a new switch is added to the cluster, a community string is created for it from the community string for the cluster. Only the first read-only and read-write community strings are propagated to the cluster.

Figure 4-9 SNMP Manager

The screenshot shows the SNMP Manager configuration window with three main sections: SNMP Agent, Community Strings, and Trap Managers. Annotations with arrows point to specific elements:

- SNMP Agent:** An arrow points to the Enable radio button. Text: "Click one to allow or disallow SNMP applications access to the switch."
- Community Strings:**
 - An arrow points to the Name input field. Text: "Enter a character string to authenticate SNMP requests."
 - An arrow points to the Read Only radio button. Text: "Click to display MIB object information."
 - An arrow points to the Read/Write radio button. Text: "Click to display and set MIB objects."
 - An arrow points to the Current Community Strings list, which contains "private RW" and "public RO".
- Trap Managers:**
 - An arrow points to the IP Address input field. Text: "Enter the IP address of PC or workstation to receive traps."
 - An arrow points to the Community input field. Text: "Enter a character string to act as a password for the trap manager."
 - An arrow points to the Current Trap Managers list, which contains "172.20.245.5".

At the bottom of the window are buttons for OK, Cancel, and Help. A vertical ID number "22226" is located at the bottom right corner of the window.

Enabling Traps

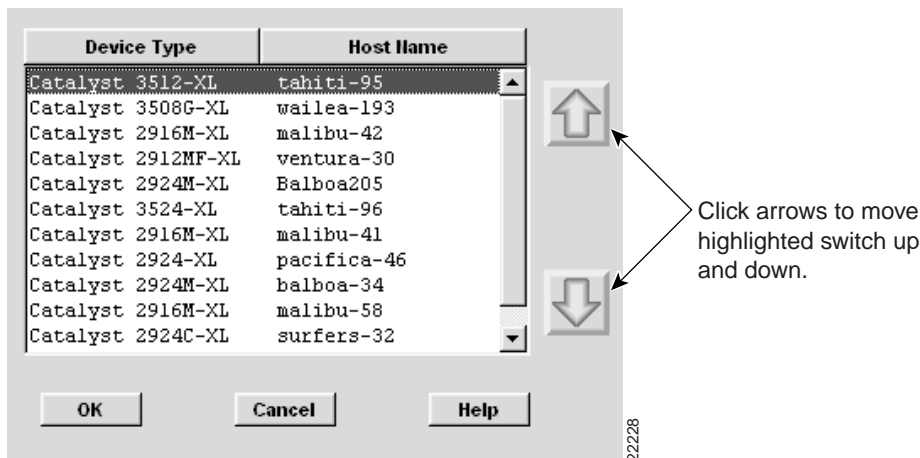
Traps are system alerts that the switch generates when certain events occur. The command switch forwards traps from member switches to the SNMP management station. From this page you can enable the switch to generate the following traps:

Config	Generate a trap when the switch configuration changes.
TTY	Generate a trap when the switch starts a CLI session
VTP	Generate a trap when the VLAN Trunk Protocol (VTP) changes (Enterprise Edition Software only).
SNMP	Generate the switch SNMP traps.
C2900/C3500	Generate the Catalyst 2900 XL and Catalyst 3500 XL traps. See Chapter 3, “Managing Your Switches” for the traps generated to support specific switch features.
VLAN Membership	For Enterprise Edition Software, generate a trap when the VLAN Membership Policy Server (VMPS) changes.

Rearranging the Order of the Switches

You can arrange the order in which switches are displayed by Cluster Manager. Select a device in the Device Arrangement page shown in Figure 4-10, and use the arrows to move it up or down in the list. Click **OK** when finished.

Figure 4-10 Device Arrangement



Displaying Link Utilization Graphs

You can use Cluster Management to display real-time graphs that can help you analyze traffic patterns and identify problems with individual links. You can start a graph from Cluster Builder, Cluster Manager, or Cluster View. To display a link graph in Cluster Builder or Cluster View, click a link and then right-click to display the pop-up menu. Select **Link Graph**. To display a link graph in Cluster Manager, left-click a port and right-click to display the pop-up menu. Select **Link Graph**.

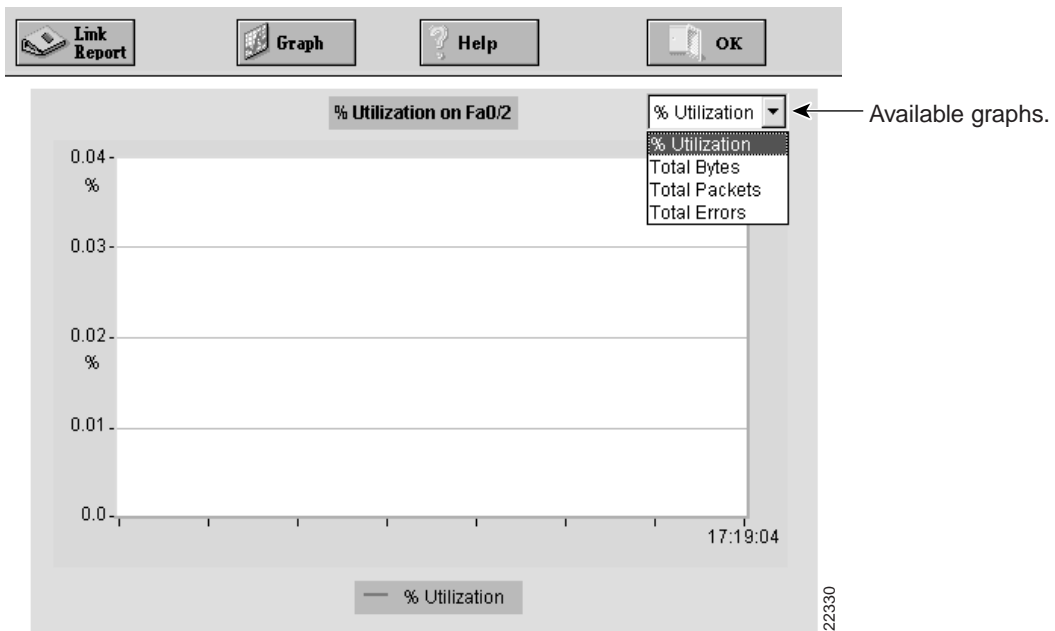
A graph runs as a separate browser session and can run in the background without interrupting the original session. The host name of the switch is displayed at the top of the browser window. The link port number is displayed above the graph itself.

When the graph window is displayed, use the drop-down menu in the upper right corner to select the data you want to present, as shown in Figure 4-11.

Select one of the following graphs from the drop-down menu:

- Percent utilization (Figure 4-11)
- Total number of bytes sent and received (Figure 4-12)
- Packets sent and received, including broadcast and multicast packets
- Total errors, including error packets and dropped packets

Figure 4-11 Link Graph



Displaying the Percent Utilization

This graph (Figure 4-11) displays the percentage of the maximum bandwidth in use by the port number displayed on the graph. The IP address of the switch is displayed at the very top of the window.

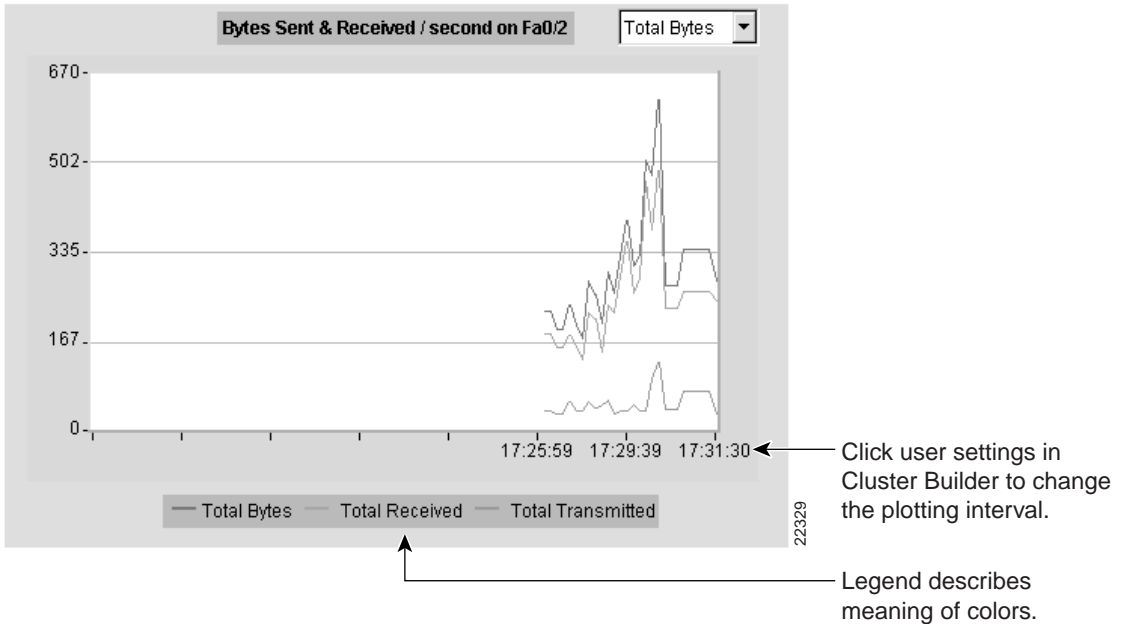
Displaying Total Bytes Sent and Received on a Link

This graph (Figure 4-12) displays the number of bytes sent and received by the port number displayed on the graph.

The following colors represent three different graphs:

- Blue—Total number of bytes sent and received on the port
- Red—Total number of bytes sent on the port
- Black—Total number of bytes received on the port

Figure 4-12 Total Bytes Sent and Received



Displaying Total Number of Packets Sent on a Link

This graph displays the number of packets sent and received by the port number displayed on the graph. The following colors represent the two graphs:

- Blue—Total number of packets sent and received on the port
- Red—Total number of broadcast and multicast packets sent and received on the port

Displaying the Total Errors on a Link

This graph displays the total number of errors sent and received by the port number displayed on the graph. The following colors represent the two graphs:

- Blue—Total number of packets with errors sent and received on the port
- Red—Total number of packets dropped by the port

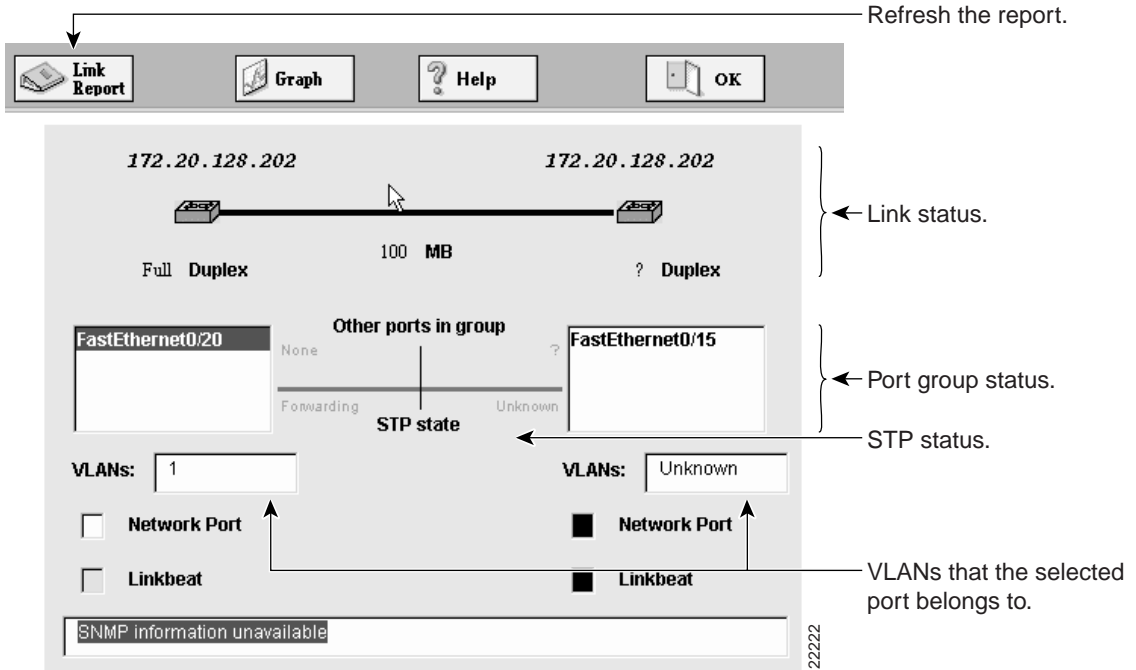
Displaying Reports

Cluster Management can extract real-time information from cluster switches and present it in the form of device and link reports. This section describes the variety of reports that Cluster Management can generate.

Displaying the Link Report

Figure 4-13 shows the link report that you can create by selecting a link and right-clicking on the pop-up menu to select **Link Report**.

Figure 4-13 Link Report



Displaying Device Reports

To display a device report, click the device, right-click to display the pop-up window, and select **Device Report**.

Each device report displays with a drop-down menu in the upper right corner. From the drop-down menu, you can display the following reports:

- Config Information (Figure 4-14)
- System Information (Figure 4-15)
- Port Information (Figure 4-16)

Figure 4-14 Config Information Device Report

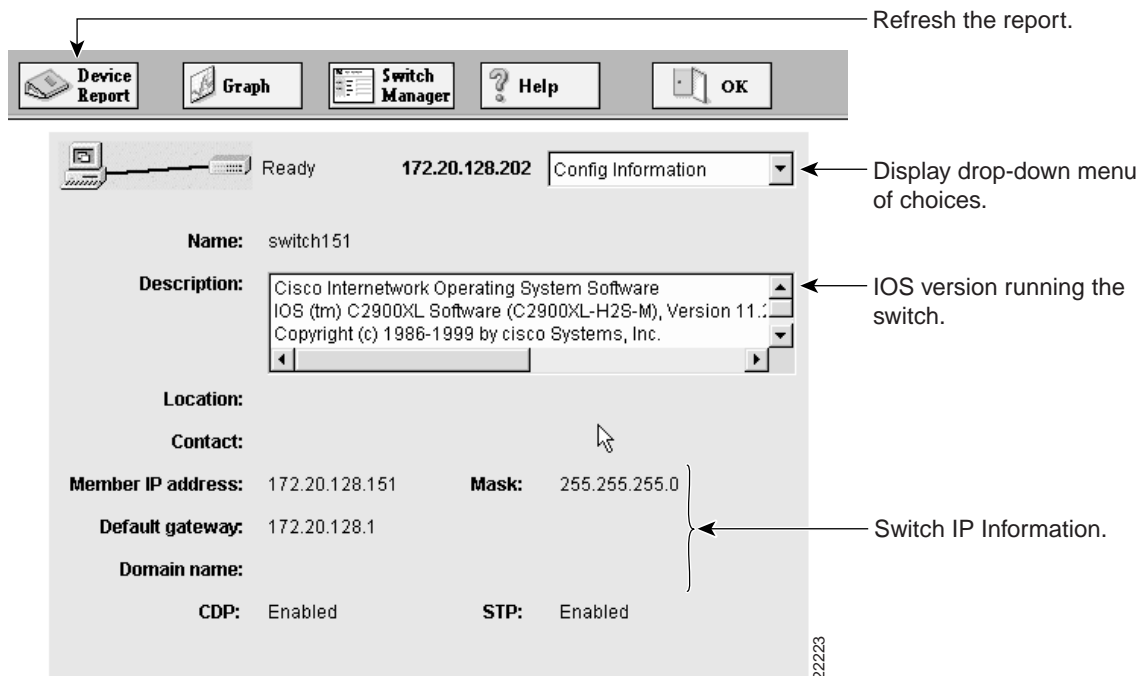
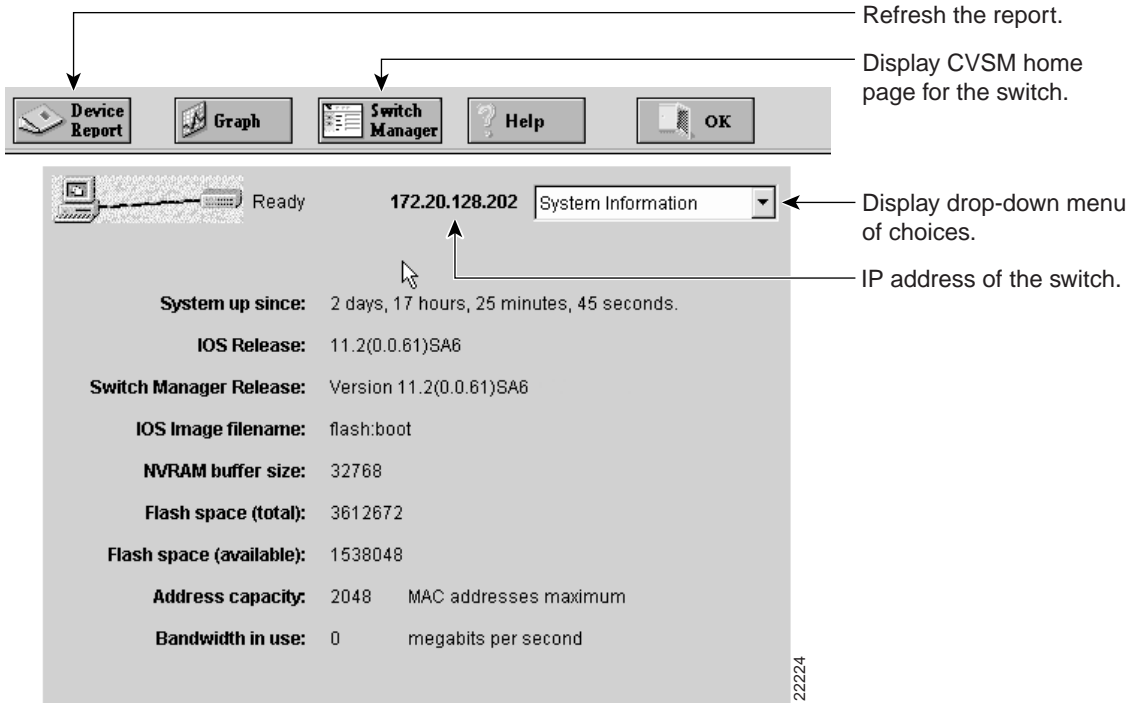


Figure 4-15 System Information Device Report



Displaying Reports

Figure 4-16 Port Information Device Report

