CHAPTER 3

Managing Your Switches

You can use the IOS Release 11.2(8)SA6 software to manage a single switch, a group of switches that are managed individually, or a cluster of switches that is managed through a single IP address. You can use any of the management interfaces to manage a switch or cluster. This chapter describes the switching features provided by Release 11.2(8)SA6 and how you can change them. For descriptions of the network-management features and clustering, see Chapter 4, “Managing Clusters of Switches.”

The graphical user interface of Cisco Visual Switch Manager (CVSM) is the primary focus of this chapter. You can use this interface to monitor a live image of the switch, reconfigure ports and other features, and upgrade the switch software.

Cisco IOS command-line interface (CLI) procedures are included for many tasks in this chapter. However, this guide describes only the use of IOS commands that have been created or changed for use with Catalyst 2900 XL and Catalyst 3500 XL switches. These commands are further described in the *Cisco IOS Desktop Switching Command Reference*. For information on other IOS Release 11.2(8) commands, see the IOS documentation set available from the CCO home page by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 11.2**.

Note How-to information for CVSM is in the online help available from all CVSM pages.

This chapter also describes the Cisco Switch Network View, hereafter called Network View, an HTML tool that displays a map of the devices that are connected to your switch. From this map you can display the CVSM interface for the other supported switches.

Default Settings and Where to Change Them

You can configure the features of this IOS release by using any of the available interfaces. Table 3-1 lists the most important features, their defaults, and where they are described in this guide.

Table 3-1 Default Settings and Where to Find Them

Feature	Default Setting	HTML Interface or Menu Option	IOS CLI Procedure
Network Management			
Creating clusters	None	Cluster Builder "Creating Clusters" section on page 4-2	"CLI Commands for Creating a Cluster" section on page 4-6
Removing cluster members	None	Cluster Manager "Managing Clusters" section on page 4-11	"CLI Commands for Removing a Cluster Member" section on page 4-9
Upgrading cluster software	Enabled	Cluster Manager "Upgrading Software for a Group of Switches" section on page 4-16	"CLI Commands for Upgrading Member Switches" section on page 4-18
Displaying reports	Enabled	Cluster Manager, Cluster Builder, Cluster View "Displaying Reports" section on page 4-26	–
Device Management			
Switch IP address, subnet mask, and default gateway	0.0.0.0	System>IP Management "Setting the System Date and Time" section on page 3-36	"CLI Commands for Assigning IP Information to the Switch" section on page 3-42
Cisco Discovery Protocol (CDP)	Enabled	Device>Cisco Discovery Protocol "Configuring the Cisco Discovery Protocol" section on page 3-59	Documentation set for Cisco IOS Release 11.2(8) on CCO
Address Resolution Protocol (ARP)	Enabled	System>ARP Table "Managing the ARP Table" section on page 3-47	Documentation set for Cisco IOS Release 11.2(8) on CCO

Table 3-1 Default Settings and Where to Find Them

Feature	Default Setting	HTML Interface or Menu Option	IOS CLI Procedure
System Time Management	None	System>System Time Management “Setting the System Date and Time” section on page 3-36	Documentation set for Cisco IOS Release 11.2(8) on CCO
Static address assignment	None assigned	Security>Address Management “Adding and Removing Static Addresses” section on page 3-52	“CLI Commands for Adding Static Addresses” section on page 3-54
Cisco Switch Network View	Enabled	“Managing Switches via Switch Network View” section on page 3-6	–
VLAN membership	Static access ports in VLAN 1	VLAN>VLAN Membership “Assigning Ports to VLANs” section on page 3-74	“CLI Commands for Assigning Static Access Ports to a VLAN” section on page 3-74
Performance			
Autonegotiation of duplex mode	Enabled	Port>Port Configuration “Configuring Port Parameters” section on page 3-19	“CLI Procedure for Setting Speed and Duplex Parameters” section on page 3-20
Autonegotiation of port speeds	Enabled	Port>Port Configuration “Configuring Port Parameters” section on page 3-19	“CLI Procedure for Setting Speed and Duplex Parameters” section on page 3-20
Flooding Control			
Broadcast storm control	Disabled	Port>Flooding Controls “Enabling Broadcast Storm Control” section on page 3-29	“CLI Commands for Enabling Broadcast Storm Control” section on page 3-29
Flooding unknown unicast and multicast packets	Enabled	Port>Flooding Controls “Blocking Flooded Traffic on a Port” section on page 3-30	“CLI Commands for Blocking Flooded Traffic on a Port” section on page 3-30
Network port	Disabled	Port>Flooding Controls “Enabling a Network Port” section on page 3-28	“CLI Commands for Enabling a Network Port” section on page 3-28

Table 3-1 Default Settings and Where to Find Them

Feature	Default Setting	HTML Interface or Menu Option	IOS CLI Procedure
Cisco Group Management Protocol (CGMP)	Enabled	Device>Cisco Group Management Protocol “Controlling IP Management Packets via CGMP” section on page 3-62	“CLI Commands for Enabling the CGMP Fast Leave Option” section on page 3-63
Network Redundancy			
Spanning-Tree Protocol	Enabled	Device>Spanning-Tree Protocol “Configuring Spanning-Tree Protocol” section on page 3-65	“CLI Commands for Enabling STP Port Fast” section on page 3-72
Port grouping	None assigned	Port>Port Grouping (EC) “Creating EtherChannel Port Groups” section on page 3-21	“CLI Commands to Create EtherChannel Port Groups” section on page 3-24
Diagnostics			
SPAN port monitoring	Disabled	Port>Switch Port Analyzer (SPAN) “Enabling Switch Port Analyzer” section on page 3-24	See the documentation set for Cisco IOS Release 11.2(8) on CCO
Console, buffer, and file logging	Disabled	Fault>Logging Config “Configuring the Switch to Log Information” section on page 3-78	Documentation set for Cisco IOS Release 11.2(8) on CCO
Security			
Password	None	Visual Switch Manager Home “Changing the Password” section on page 3-12	“Recovering from a Lost or Forgotten Password” section on page 5-4
Addressing security	Disabled	Security>Address Management “Adding Secure Addresses” section on page 3-51	“CLI Commands for Adding Secure Addresses” section on page 3-52
Trap manager	0.0.0.0	System>SNMP Configuration “Adding Trap Managers” section on page 3-45	Documentation set for Cisco IOS Release 11.2(8) on CCO

Table 3-1 Default Settings and Where to Find Them

Feature	Default Setting	HTML Interface or Menu Option	IOS CLI Procedure
Community strings	public	System>SNMP Configuration “Entering Community Strings” section on page 3-45	Documentation set for Cisco IOS Release 11.2(8) on CCO
Port security	Disabled	Security>Port Security “Enabling Port Security” section on page 3-56	Documentation set for Cisco IOS Release 11.2(8) on CCO

Managing Configuration Conflicts

Certain combinations of port features conflict with one another. For example, if you define a port as the network port for a VLAN, all unknown unicast and multicast traffic is flooded to the port. You could not enable port security on the network port because a secure port limits the traffic allowed on it. In Table 3-2, **no** means that the two referenced features are incompatible.

If you try to enable incompatible features by using CVSM, CVSM issues a warning message and prevents you from making the change. Reload the web page to refresh CVSM.

Table 3-2 Incompatible Features

	ATM Port[1]	Port Group	Port Security	SPAN Port	Multi-VLAN Port	Network Port[2]
ATM Port	–	No	No	No	No	No
Port Group	No	–	No	No	Yes	Yes
Port Security	No	No	–	No	No	No
SPAN Port	No	No	No	–	No	No
Multi-VLAN Port	No	Yes	No	No	–	Yes
Network Port	No	Yes (source-based only)	No	No	Yes	–

[1] Catalyst 2900 XL only.

[2] Cannot be used in a cluster.

Saving Changes to the Startup Configuration

The configuration file that loads when the switch is restarted is in Flash memory. This configuration in this file is not necessarily the same as the running configuration. If you want the running (current) configuration to be used when the switch restarts, use CVSM or the CLI to save the configuration file. This procedure is described for CVSM in the "Reloading and Upgrading the Switch Software" section on page 3-31. It is described for the CLI in the "Working with Files in Flash Memory" section on page 2-31.

Managing Switches via Switch Network View

This section describes the switch Network View, an application that extends web-based network management to the other devices in your network. By exchanging Cisco Discovery Protocol (CDP) messages with attached CDP-enabled devices, a Network View switch is able to graphically display a surrounding star topology that can consist of Catalyst 2900 and Catalyst 3500 series XL switches and Cisco edge devices.

Network View is an alternative to the cluster that you can create by using Cluster Management. Each Network View member needs to be assigned its own IP address. A Network View stack differs from a cluster in that each member has its own IP address assigned to it. In addition, a Network View stack must be in a star topology and does not support daisy-chained switches.

Understanding a Network View Stack

The center node in a star topology acts as a *primary* switch in Network View. Up to four directly connected supported switches can be stack members. These switches can be displayed in a consolidated physical view called the *visual stack*. You can access device and link information from the Network View page and the Visual Stack page.

If more than four switches are connected, Network View displays only the four connected to the lowest port numbers of the primary switch. All other devices are considered edge devices. A star topology with the primary switch in the center ensures the most complete view of the network.

To run Network View, all stack members must be running Cisco IOS Release SA6 or later and the corresponding CVSM release. In addition, you need to enable SNMP and set the community string to **public** on all stack members.

For a complete description of the Network View interface, see “Using Switch Network View” section on page 2-11.

Displaying the Network View Page

If you have not enabled a command switch, the Network View page (Figure 3-1) displays a map of the devices and links that are directly connected to your switch. From this page, you can display switch-connection information, device reports, and link reports. This page also displays Cisco routers, switches, hubs, and Cisco Micro Web Servers, but these devices must be directly attached to one of the supported switches. Other devices using CDP display as generic edge devices.

Note Before starting Network View, make sure you are using a supported browser. For more information, see the “Hardware and Software Requirements” section on page 2-2.

Follow these steps to display the Network View page:

Step 1 On the Switch Manager home page, click **Switch Network View**.

Step 2 When prompted, enter the enable password for each switch in the stack. You do not need to enter a user name.

Displaying Switch Connection Information

Figure 3-2 shows the information that you can display about the switches being managed by Network View. Click on the Switch Manager button on the Network View page to display this table.

Figure 3-1 Switch Network View Page

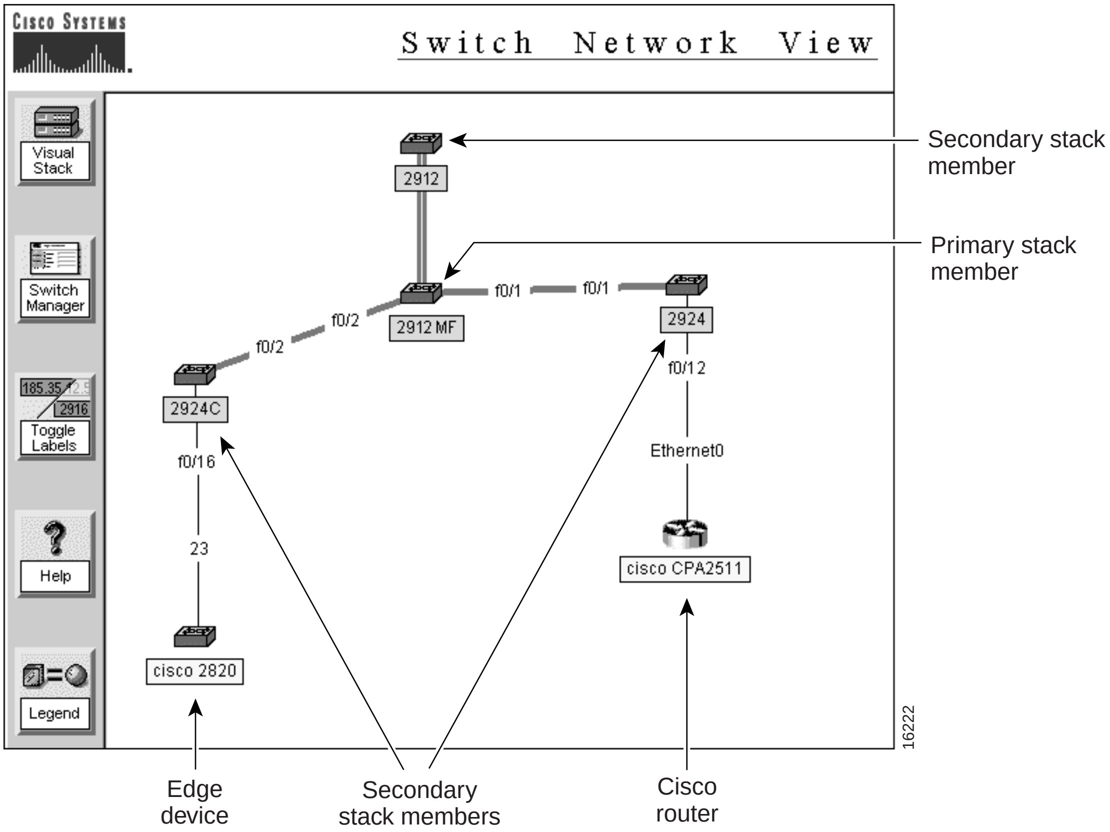
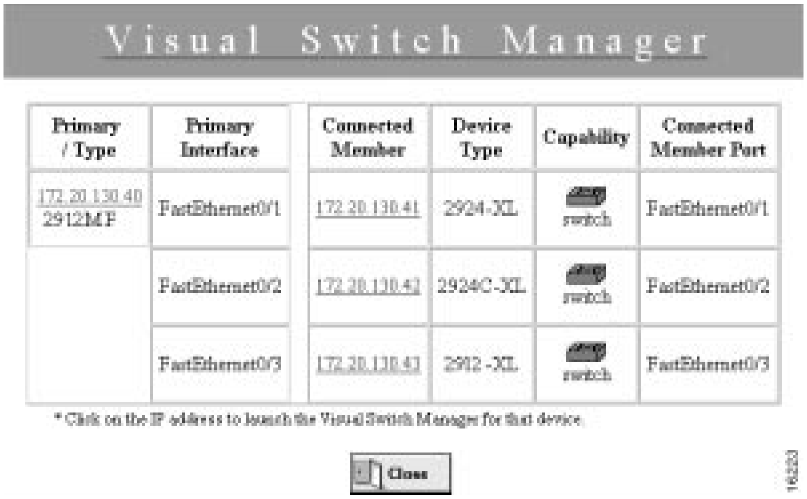


Figure 3-2 Visual Switch Manager Connection Information



Visual Switch Manager

Primary / Type	Primary Interface	Connected Member	Device Type	Capability	Connected Member Port
172.20.130.40 2912MF	FastEthernet0/1	172.20.130.41	2924-XL	switch	FastEthernet0/1
	FastEthernet0/2	172.20.130.42	2924C-XL	switch	FastEthernet0/2
	FastEthernet0/3	172.20.130.43	2912 -XL	switch	FastEthernet0/3

* Click on the IP address to launch the Visual Switch Manager for that device.

Displaying the Cisco Visual Stack

The visual stack is an image of up to four Catalyst 2900 series XL or Catalyst 3500 series XL switches (Figure 3-3) with the primary switch at the top. This stack contains the same switches as those on the Network View page, which displays the primary switch in the middle and stack members connected to it. The stack images display real-time information about the switches and their ports. You can use the stack to monitor port status, check port speed and duplex settings, configure switch ports, and start the CVSM software.

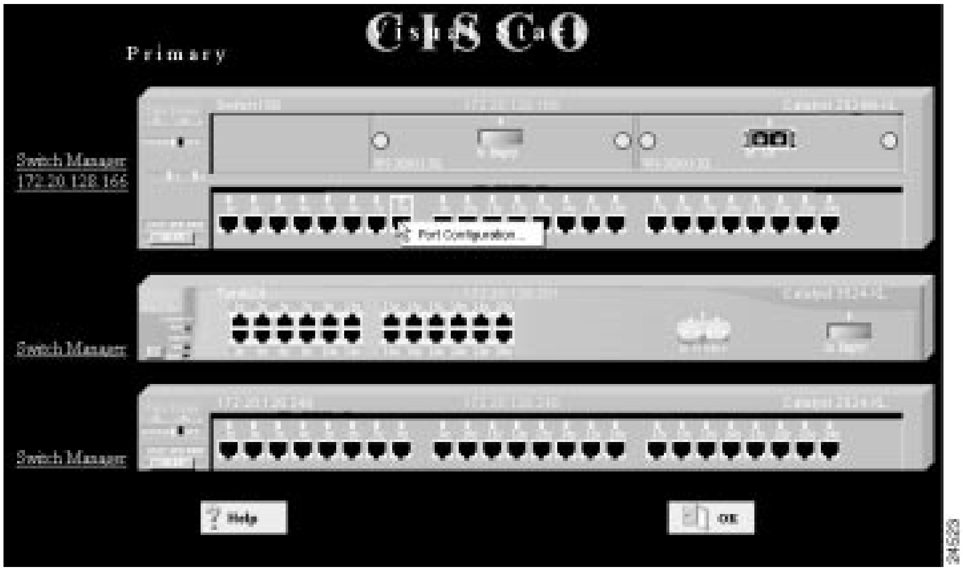
Follow these steps to display the Visual Stack page:

Step 1 Display the Network View page as described in the “Displaying the Network View Page” section on page 3-7.

Step 2 Click **Visual Stack** in the upper-left corner of the page.

The visual stack displays in a separate browser window (see Figure 3-3).

Figure 3-3 Visual Stack



Monitoring Port Status

The visual stack shows LED colors to depict the port status:

- Green—port is active.
- Blue—port is inactive.
- Amber—port is disabled administratively or by STP.

Checking Port Speed and Duplex Settings

To check the transmission speed settings for all switch ports, click **MODE**, and highlight **SPD** (speed). Blue means 10 Mbps; green means 100 Mbps.

To check the duplex setting, click **MODE,** and highlight **FDUP** (full-duplex). Blue means half-duplex mode; green means full-duplex mode.

Configuring Switch Ports

On the visual stack, click on a port and right-click to display the pop-up menu. Select **Port Configuration**. The Port Configuration pop-up window shows the port settings and status. Select **Enable** to enable or disable the port and STP Port Fast setting, and select a speed and duplex setting from the drop-down lists. This window is the same as the one described in the "Configuring Ports on the Switch Home Page" section on page 3-14.

In addition, you can configure multiple ports as a group. To do so, press **Ctrl** and left-click the ports, and then right-click the selected ports and select Port Configuration from the pop-up menu.

Accessing CVSM

The visual stack displays the IP address of each switch next to the switch image. Click the IP address to open a separate browser window displaying the CVSM home page for that switch. End the browser session when you want to return to the visual stack.

Note If you access the CVSM to configure a stack member and then redisplay Network View, that stack member becomes the primary switch. The Network View displays devices in a different arrangement, and a stack member could become an edge device.

Managing Your Switch via CVSM

You access CVSM through one of the supported browsers described in the "Hardware and Software Requirements" section on page 2-2. Ensure that you have the browser configured correctly before starting CVSM.

Using the Switch Home Page

The Cisco Visual Switch Manager Home page (Figure 3-4) is always displayed when you click **Visual Switch Manager** on the Cisco Systems Access page. All the CVSM pages have a Home button you can click to return to this page.

Use this page to perform the following tasks:

- Changing the password
- Enabling the switch as a command switch
- Displaying Cluster Management and Network View
- Monitoring switch LEDs
- Configuring ports

Changing the Password

Changing the password from this page breaks your connection with the switch, and the browser prompts you for the new password. Click **Help** for the complete procedure. If you have forgotten your password, see the "Recovering from a Lost or Forgotten Password" section on page 5-4.

Enabling the Switch as a Command Switch

If the switch is command-capable, use this page to enable it as the command switch and to name the cluster. The Cluster Management button displays on the home page after the command switch is enabled, and the cluster name appears in Cluster View with the cluster icon. Table 1-1 in Chapter 1, "Introduction," lists the switches that are able to be command switches and those that can be enabled by a software upgrade.

Using the Switch Image to Monitor and Configure the Switch

The CVSM home page refreshes the image of the switch every 30 seconds. Besides using it to configure the features listed in this section, you can use the switch images in Cluster Manager to display VLAN membership information and detailed information about the links between switches. For more information on monitoring the switch via a web interface, see the Chapter 4, “Managing Clusters of Switches.”

Monitoring the Ports

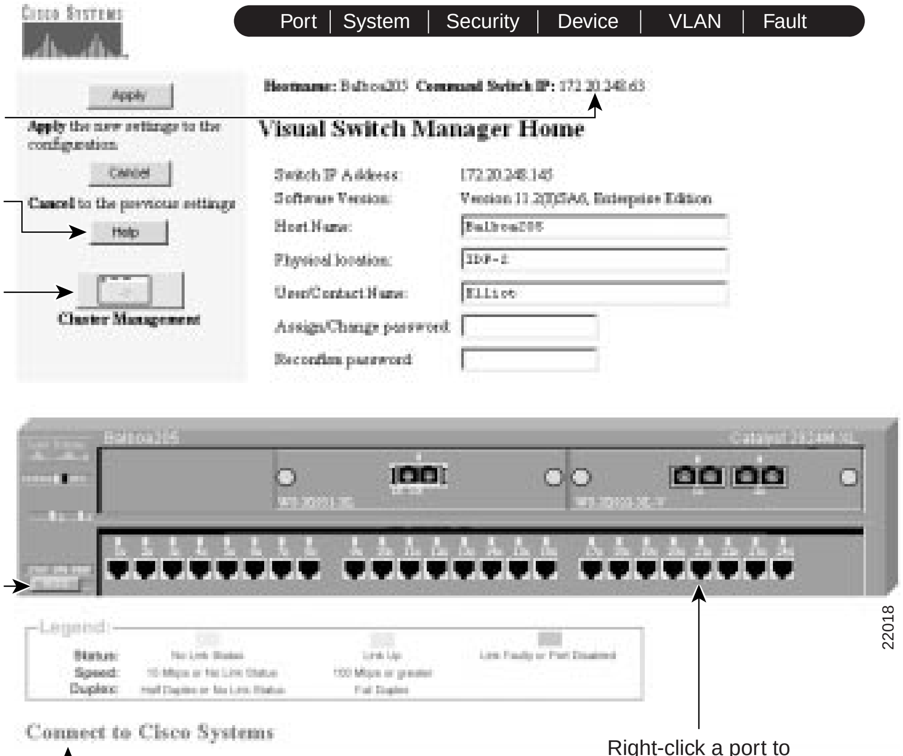
The LEDs on the switch image present the same information as the actual LEDs, but they use colors instead of the on/off methods used on the switch front panel. Click the Mode button to highlight STAT (status), SPD (speed), or FDUP (duplex), thus changing the information conveyed by the port LEDs. The legend under the image describes the meaning of the colors in each mode.

Monitoring Other Switch LEDs

The other LEDs function as follows:

- The System LED displays the status of the switch.
- The RPS LED lights when a Cisco RPS is attached.
- The 1 or 2 LED is on when a module is installed in a modular switch model.

Figure 3-4 CVSM Home Page



Hostname: Balboa205 **Command Switch IP:** 172.20.248.63

Visual Switch Manager Home

Apply the new settings to the configuration.

Cancel to the previous settings

Switch IP Address:	172.20.248.145
Software Version:	Version 11.2(8)SA6, Enterprise Edition
Host Name:	Balboa205
Physical location:	IDF-2
User/Contact Name:	Elliot
Assign/Change password:	
Reconfirm password:	

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

Shows the command switch defined in Cluster Builder.

Provides procedures and detailed field descriptions.

Click to display the switch cluster.

Click Mode to change the meaning of the port LEDs to those described in the Legend. The options are STAT (status), SPD (speed), and FDUP (duplex).

Click here to display the Cisco Connection Online (CCO) home page.

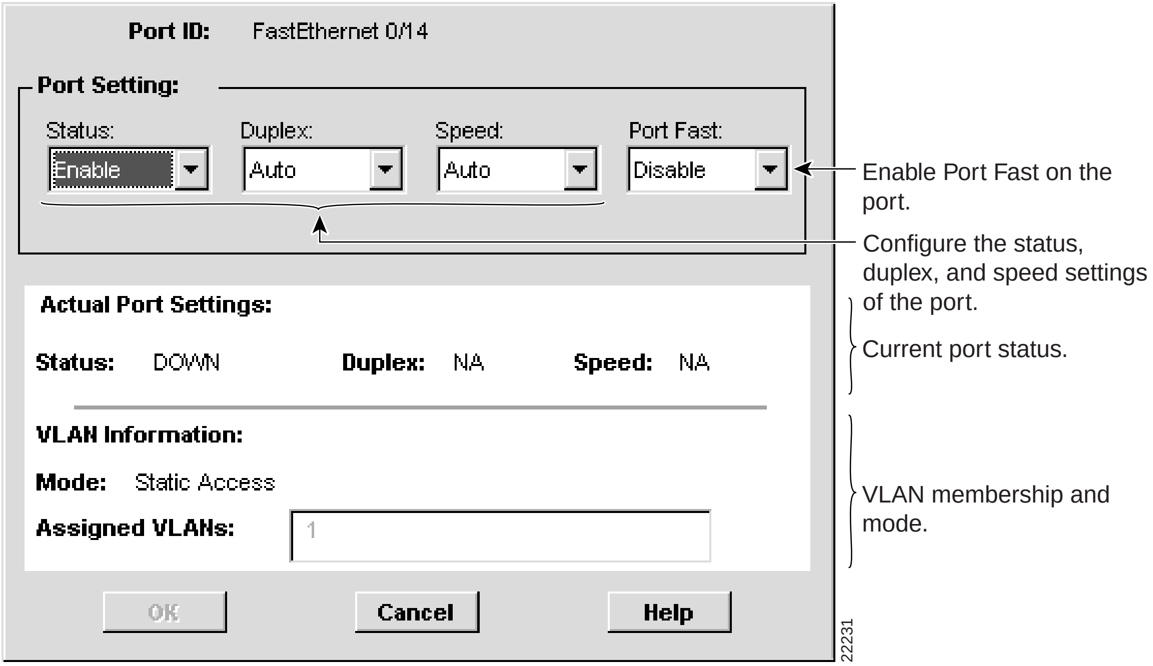
Right-click a port to configure speed and duplex settings and disable the port or STP Port Fast feature.

Configuring Ports on the Switch Home Page

To configure a port, left-click on it and then right-click to display the pop-up menu. Select **Port Configuration**. Press+ **Ctrl** and left-click the ports to select more than one at a time. The dialog box shown in Figure 3-5 displays the same information and supports the same changes as the Port Configuration page. The live LEDs on the image of the switch reflect any changes you make.

This IOS release supports 10/100, Gigabit Ethernet, ATM, and Catalyst GigaStack Gigabit Interface Converters (GBICs). See the “Configuring Port Parameters” section on page 3-19 for defaults and guidelines for configuring the different types of ports.

Figure 3-5 Port Configuration Dialog Box



Port ID: FastEthernet 0/14

Port Setting:

Status: Enable

Duplex: Auto

Speed: Auto

Port Fast: Disable

Actual Port Settings:

Status: DOWN **Duplex:** NA **Speed:** NA

VLAN Information:

Mode: Static Access

Assigned VLANs: 1

Enable Port Fast on the port.

Configure the status, duplex, and speed settings of the port.

Current port status.

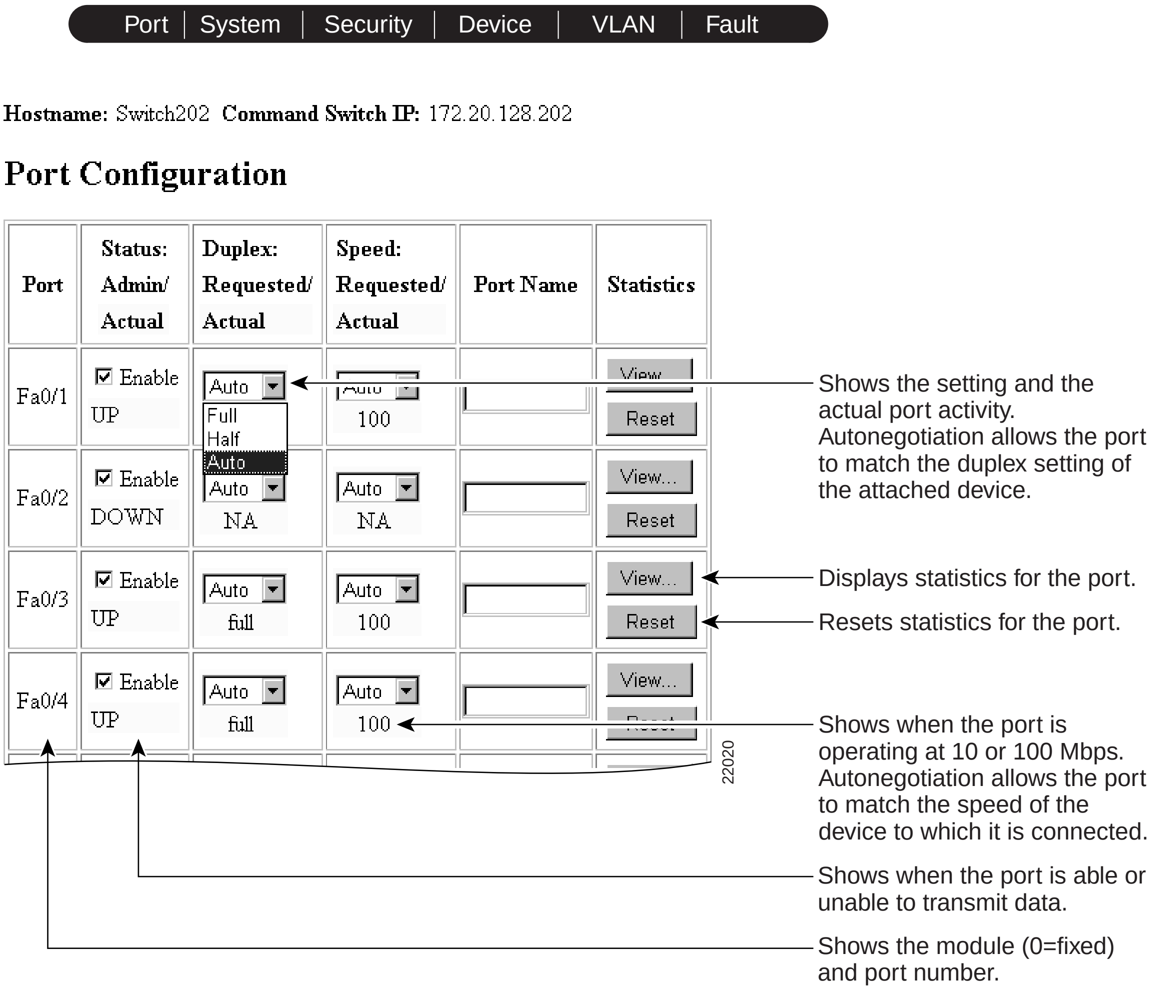
VLAN membership and mode.

Configuring Ports

Use this page to enable and disable ports and to set the duplex, speed and Port Fast parameters. Select **Port>Port Configuration** from the menu bar.

Figure 3-6 shows the Port Configuration page, and Table 3-3 describes the meaning of column headings and fields. The “Configuring Port Parameters” section on page 3-19 contains guidelines for you to use when using this page.

Figure 3-6 Port Configuration Page



Hostname: Switch202 **Command Switch IP:** 172.20.128.202

Port Configuration

Port	Status: Admin/ Actual	Duplex: Requested/ Actual	Speed: Requested/ Actual	Port Name	Statistics
Fa0/1	☑ Enable UP	Auto Full Half Auto	Auto 100		View... Reset
Fa0/2	☑ Enable DOWN	Auto NA	Auto NA		View... Reset
Fa0/3	☑ Enable UP	Auto full	Auto 100		View... Reset
Fa0/4	☑ Enable UP	Auto full	Auto 100		View... Reset

Shows the setting and the actual port activity. Autonegotiation allows the port to match the duplex setting of the attached device.

Displays statistics for the port.

Resets statistics for the port.

Shows when the port is operating at 10 or 100 Mbps. Autonegotiation allows the port to match the speed of the device to which it is connected.

Shows when the port is able or unable to transmit data.

Shows the module (0=fixed) and port number.

Table 3-3 Port Configuration Parameters

Port	Displays Fa (Fast Ethernet), Gi (Gigabit Ethernet), or AT (ATM); the module number: 0 (fixed), 1 (right slot), or 2 (left slot); and the port number. In Figure 3-5, the port is a fixed port (0) and port number 14: Fa0/14. **Note** The port numbers for the double-row connectors on the Catalyst 3500 series XL switches increment from top to bottom.
Status: Admin/Actual	Enables or disable the port. The field also displays the current port status.
Duplex: Requested/Actual	Displays the current duplex setting. You can 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: Requested/Actual	Displays the current speed setting. You can set a 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 Name	Names the port or describes how it is connected.
Statistics	Displays transmit and receive statistics for the port. Click **Reset** to clear the statistics and close the statistics window.
Flow Control	Enables or disables flow control on Gigabit Ethernet ports. Flow control enables the connected Gigabit Ethernet ports to control traffic rates during congestion. If one port experiences congestion and cannot receive any more traffic, it notifies the other port to stop transmitting until the condition clears. Select **Symmetric** when you want the local port to perform flow control of the remote port only if the remote port can also perform flow control on the local port. Select **Asymmetric** when you want the local port to perform flow control on the remote port. For example, if the local port is congested, it notifies the remote port to stop transmitting. This is the default setting Select **Any** when the local port can support any level of flow control required by the remote port. This setting is the default. Select **None** to disable flow control on the port. This field is displayed only when a Gigabit Ethernet port is present; it does not apply to Fast Ethernet or ATM ports.

Configuring Port Parameters

The Port Configuration page displays the Requested and Actual settings for each port. A port connected to a device that does not support the requested setting or that is not connected to a device can cause the Requested and Actual settings to differ.

Caution It is possible to reconfigure the port through which you are managing the switch. STP reconfiguration could cause a temporary loss of connectivity.

Follow these guidelines when configuring the duplex and speed settings:

- Gigabit Ethernet ports are always set to a speed of 1000 but can negotiate full- or half-duplex with the attached device.
- ATM ports are always set to full and do not autonegotiate duplex or speed settings.
- Gigabit Ethernet ports that fail to match the settings of an attached device lose connectivity and do not generate statistics.
- GigaStack-to-GigaStack stack connections operate in half-duplex mode, and GigaStack-to-GigaStack point-to-point connections operate in full-duplex mode.
- If STP is enabled, the switch can take up to 30 seconds to check for loops when a port is reconfigured. The port LED is amber while STP reconfigures.
- After you make a change, you can verify the change by clicking the port on the Home page or by using the Mode button.

Connecting To Devices That Do Not Autonegotiate

To connect to a remote 100BaseT device that does not autonegotiate, do not configure AUTO for the duplex setting on the local device. Autonegotiation of the speed setting works correctly even if the attached device does not autonegotiate.

To connect to a remote Gigabit Ethernet device that does not autonegotiate, disable Autonegotiation on the local device, and set the duplex and flow control parameters to be compatible with the other device. For more information, see the “Identifying an Autonegotiation Mismatch” section on page 5-2.

CLI Procedure for Setting Speed and Duplex Parameters

Beginning in privileged EXEC mode, follow these steps to set the speed and duplex parameters on a port:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port to be configured.	**interface** *interface*
Step 3	Enter the speed parameter for the port. You cannot enter the speed on Gigabit Ethernet or ATM ports.	**speed** {**10** | **100** | **auto**}
Step 4	Enter the duplex parameter for the port.	**duplex** {**full** | **half** | **auto**}
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries.	**show running-config**
Step 7	(Optional) Save your entry in the configuration file. This retains the configuration when the switch restarts.	**copy running-config startup-config**

For more information on IOS Release 11.2(8)SA6, see the *Cisco IOS Desktop Switching Command Reference.* The complete IOS Release 11.2(8) documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 11.2**.

Creating EtherChannel Port Groups

Use the Port Group (EtherChannel) page (see Figure 3-8) to create Fast EtherChannel and Gigabit EtherChannel port groups. These port groups act as single logical ports for high-bandwidth connections between switches or between switches and servers.

Note You can create port groups of Gigabit Ethernet ports or 100BaseTX ports, but you cannot create a port group that contains both port speeds at the same time.

To display this page, select **Port>Port Grouping (EC)** from the menu bar.

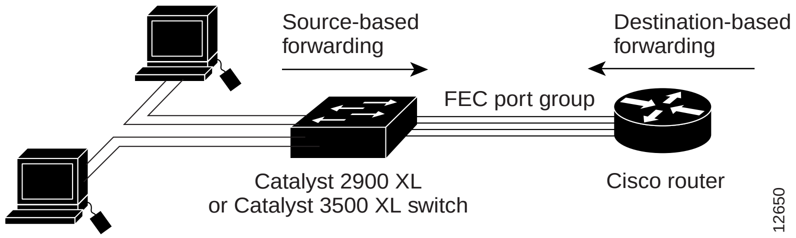
Understanding EtherChannel Port Grouping

This IOS release supports two different types of port groups: source-based forwarding port groups and destination-based forwarding port groups. Source-based forwarding ports groups distribute packets forwarded to the group based on the source address of incoming packets from ports that are not in the port group. Port groups that forward based on the source address can have as many as eight ports. Source-based forwarding is enabled by default.

Destination-based port groups distribute packets forwarded to the group based on the destination address of incoming packets from ports not in the group. Port groups that forward based on the destination address can have any number of ports.

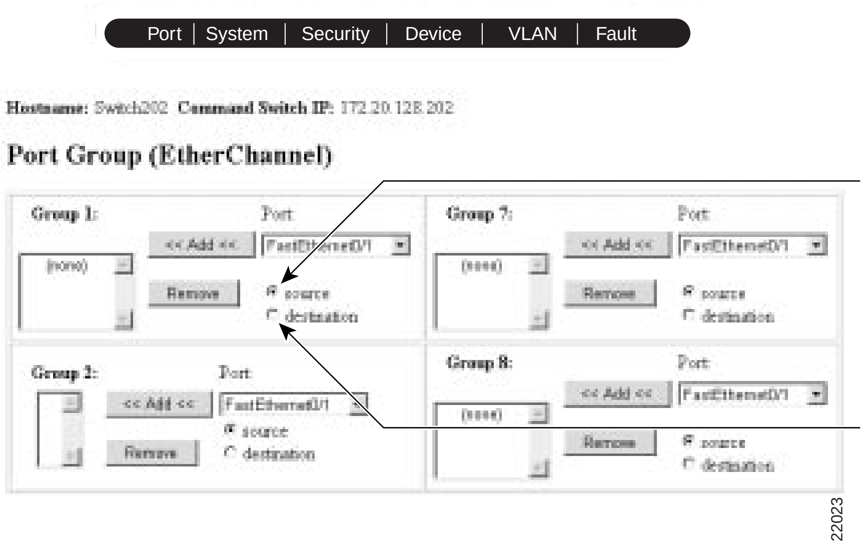
Port groups that link switches each switch, but both ends of a port group must be configured consistently. In Figure 3-7, a port group of two workstations communicates with a router. Because the router is a single-MAC address device, source-based forwarding ensures that the switch uses all available bandwidth to the router. The router is configured to forward based on destination address because the larger number of stations ensures that the traffic is evenly distributed out the port-group ports on the router.

Figure 3-7 Source-Based Forwarding



The switch treats the port group as a single logical port; therefore, when you create a port group, the switch uses the configuration of the first port for all ports added to the group. If you add a port and change the forwarding method, it changes the forwarding for all ports in the group. After the group is created, changing STP or VLAN membership parameters for one port in the group automatically changes the parameters for all ports. Each port group has one port that carries all unknown multicast, broadcast, and STP packets.

Figure 3-8 Port Group (EtherChannel)



Hostname: Switch202 **Command Switch IP:** 172.20.128.202

Port Group (EtherChannel)

Group 1: (none) Port FastEthernet0/1 ● source ○ destination

Group 7: (none) Port FastEthernet0/1 ● source ○ destination

Group 2: Port FastEthernet0/1 ● source ○ destination

Group 8: (none) Port FastEthernet0/1 ● source ○ destination

Select **source** when connecting to a router or other single-MAC address device. Maximum of 8 ports.

Select **destination** when connecting to a switch or multi-MAC address device. Any number of ports.

Port Group Restrictions on Static-Address Forwarding

The following restrictions apply to entering static addresses that are forwarded to port groups:

- If the port group forwards based on the source MAC address (the default), configure the switch to forward packets from the static address to all ports in the group. This method eliminates the chance of lost packets.
- If the port group forwards based on the destination address, configure the switch to forward packets destined for the static address to only one port in the port group. This method avoids the possible transmission of duplicate packets.

Note Check boxes for ports on the Static Address Forwarding Map appear only if they are in the same VLAN as the receiving port. For more information, see "Adding and Removing Static Addresses" section on page 3-52.

CLI Commands to Create EtherChannel Port Groups

Beginning in privileged EXEC mode, complete these tasks to create a two-port group:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port of the first port to be added to the group.	**interface** *interface*
Step 3	Assign the port to group 1 with destination-based forwarding.	**port group 1 distribution destination**
Step 4	Enter the second port to be added to the group.	**interface** *interface*
Step 5	Assign the port to group 1 with destination-based forwarding.	**port group 1 distribution destination**
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Verify your entries.	**show running-config**

For more information on IOS Release 11.2(8)SA6, see the *Cisco IOS Desktop Switching Command Reference.* The complete IOS Release 11.2(8) documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 11.2**.

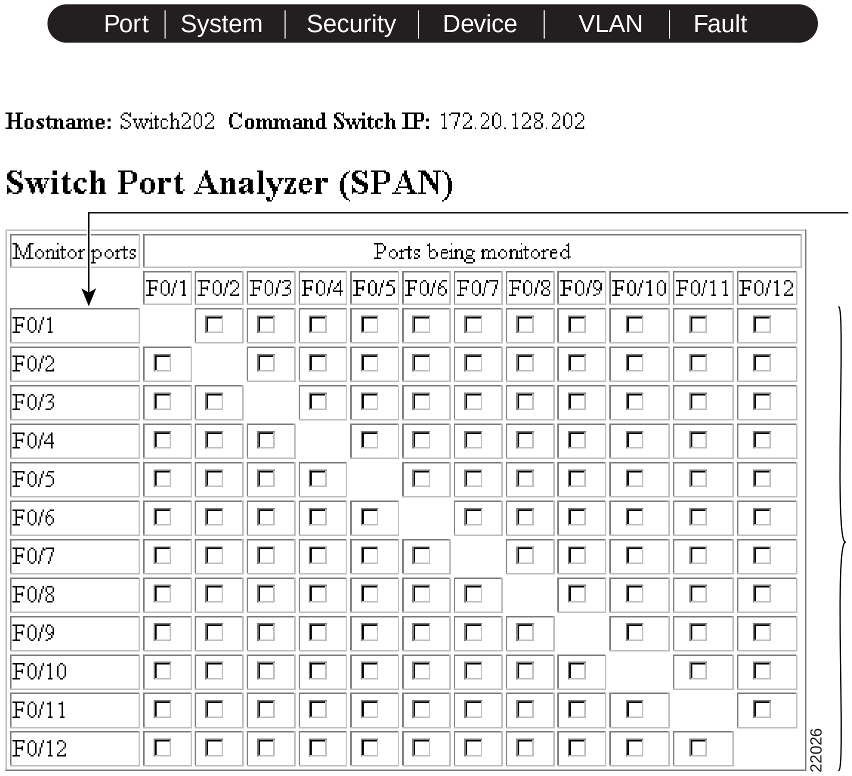
Enabling Switch Port Analyzer

Use the Switch Port Analyzer (SPAN) page (Figure 3-9) to enable port monitoring. You can monitor traffic on a given port by forwarding incoming and outgoing traffic on the port to another port in the same VLAN. A SPAN port cannot monitor ports in a different VLAN, and a SPAN port must be a static-access port. Any number of ports can be defined as SPAN ports, and any combination of ports can be monitored.

To display this page, select **Port>Switch Port Analyzer (SPAN)** from the menu bar.

For the restrictions that apply to SPAN ports, see the “Managing Configuration Conflicts” section on page 3-5.

Figure 3-9 Switch Port Analyzer (SPAN)



Hostname: Switch202 **Command Switch IP:** 172.20.128.202

Switch Port Analyzer (SPAN)

Monitor ports	Ports being monitored											
	F0/1	F0/2	F0/3	F0/4	F0/5	F0/6	F0/7	F0/8	F0/9	F0/10	F0/11	F0/12
F0/1		□	□	□	□	□	□	□	□	□	□	□
F0/2	□		□	□	□	□	□	□	□	□	□	□
F0/3	□	□		□	□	□	□	□	□	□	□	□
F0/4	□	□	□		□	□	□	□	□	□	□	□
F0/5	□	□	□	□		□	□	□	□	□	□	□
F0/6	□	□	□	□	□		□	□	□	□	□	□
F0/7	□	□	□	□	□	□		□	□	□	□	□
F0/8	□	□	□	□	□	□	□		□	□	□	□
F0/9	□	□	□	□	□	□	□	□		□	□	□
F0/10	□	□	□	□	□	□	□	□	□		□	□
F0/11	□	□	□	□	□	□	□	□	□	□		□
F0/12	□	□	□	□	□	□	□	□	□	□	□	

Monitor ports must be in same VLAN as ports being monitored.

Select up to 15 ports at a time, and click **Apply**.

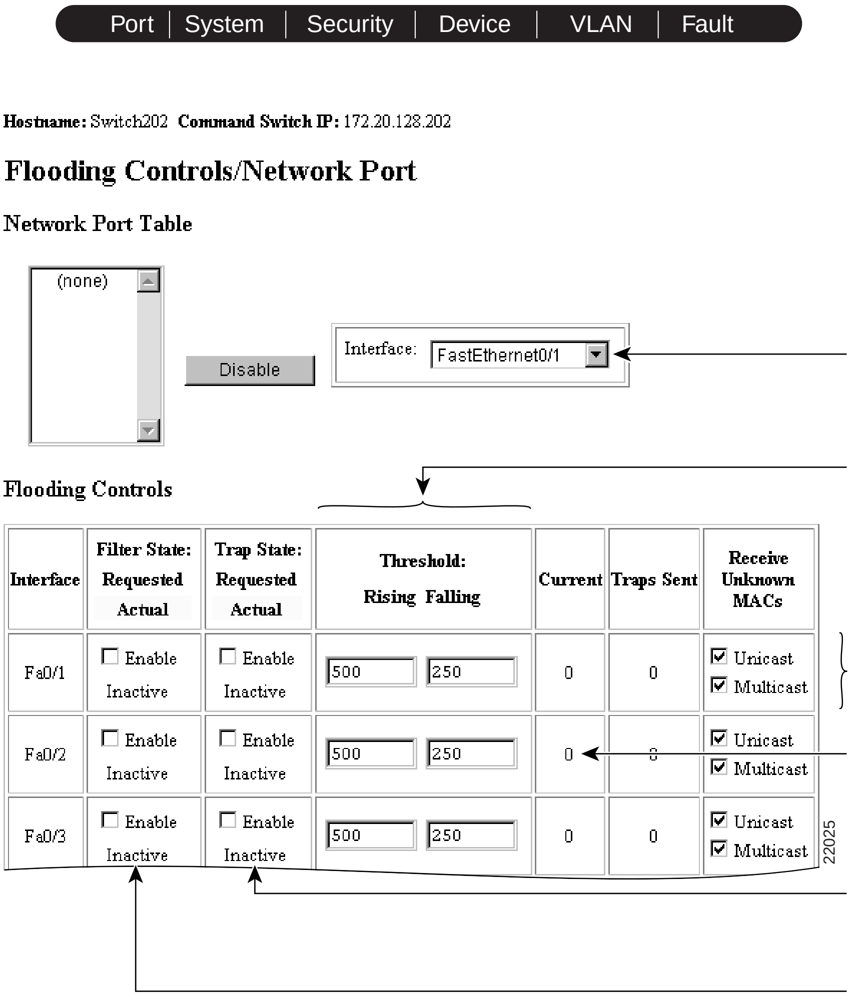
Configuring Flooding Controls

Use the Flooding Controls page (Figure 3-10) to block the forwarding of unnecessary flooded traffic. You can enable three flooding techniques from this page:

- Forward all traffic to a network port.
- Enable broadcast storm control.
- Block the forwarding of unicast and broadcast packets on a per-port basis.

To display this page, select **Port>Flooding Controls** from the menu bar.

Figure 3-10 Flooding Controls



Hostname: Switch202 **Command Switch IP:** 172.20.128.202

Flooding Controls/Network Port

Network Port Table

(none)

Disable

Interface: FastEthernet0/1

Flooding Controls

Interface	Filter State: Requested Actual	Trap State: Requested Actual	Threshold: Rising	Threshold: Falling	Current	Traps Sent	Receive Unknown MACs
Fa0/1	□ Enable Inactive	□ Enable Inactive	500	250	0	0	☑ Unicast ☑ Multicast
Fa0/2	□ Enable Inactive	□ Enable Inactive	500	250	0	0	☑ Unicast ☑ Multicast
Fa0/3	□ Enable Inactive	□ Enable Inactive	500	250	0	0	☑ Unicast ☑ Multicast

Select a port to receive all the flooded traffic in its VLAN.

Shows the start (Rising) and stop (Falling) parameters for broadcast storm control.

Deselect to disable flooding to the port.

Number of broadcast packets per second arriving on the port.

Click to send a trap when broadcast storm control starts and stops.

Click to activate broadcast storm control on the port.

Enabling a Network Port

Network ports are assigned per VLAN and can reduce flooded traffic on your network. The switch forwards all traffic with unknown destination addresses to the network port instead of flooding the traffic to all ports in the VLAN.

When you configure a port as the network port, the switch deletes all associated addresses from the address table and disables learning on the port. If you configure other ports in the VLAN as secure ports, the addresses on those ports are not aged. If you move a network port to a VLAN without a network port, it becomes the network port for the new VLAN.

You cannot change the settings for unicast and multicast flooding on a network port.

⚠ **Caution** A network port cannot link cluster members. Do not attempt to connect cluster members through a network port.

For limitations on configuring a network port, see the "Managing Configuration Conflicts" section on page 3-5.

CLI Commands for Enabling a Network Port

Beginning in privileged EXEC mode, complete these tasks to define a port as the network port:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port to be configured.	**interface** *interface*
Step 3	Define the port as the network port.	**port network**
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entry.	**show running-config**

For more information on IOS Release 11.2(8)SA6, see the *Cisco IOS Desktop Switching Command Reference.* The complete IOS Release 11.2(8) documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 11.2**.

Enabling Broadcast Storm Control

A broadcast storm occurs when a large number of broadcast packets are received. Forwarding these packets can cause the network to slow down or to time out. Broadcast storm control is configured for the switch as a whole, but operates on a per-port basis. By default, broadcast storm control is disabled.

Broadcast storm control uses specific high and low numbers of broadcast packets to block and then to restore forwarding of broadcast packets. In general, the higher the threshold, the less effective the protection against broadcast storms. The maximum half-duplex transmission on a 100BaseT link is 148,000 packets per second, but you can enter a threshold up to 4294967295 broadcast packets per second.

CLI Commands for Enabling Broadcast Storm Control

Beginning in privileged EXEC mode, follow these steps to enable broadcast-storm control.

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port to configure.	**interface** *interface*
Step 3	Enter the rising and falling thresholds.	**port storm-control** [**threshold** {**rising** *rising-number* **falling** *falling-number*}]
Step 4	Disable the port during a broadcast storm, or generate an SNMP trap when the traffic on the port crosses the rising or falling threshold.	**port storm-control filter** or **port storm-control trap**
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries.	**show port storm-control** [*interface*]

Blocking Flooded Traffic on a Port

By default, the switch floods packets with unknown destination MAC addresses to all ports. Some configurations do not require flooding. For example, a port that has only manually assigned addresses has no unknown destinations, and flooding serves no purpose. Therefore, you can disable the flooding of unicast and multicast packets on a per-port basis. Ordinarily, flooded traffic does not cross VLAN boundaries, but multi-VLAN ports flood traffic to all VLANs they belong to.

To display the page for blocking flooded traffic, select **Port>Flooding Controls** from the menu bar.

CLI Commands for Blocking Flooded Traffic on a Port

Beginning in privileged EXEC mode, follow these steps to disable the flooding of multicast and unicast packets to a port:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port to configure.	**interface** *interface*
Step 3	Block multicast forwarding to the port.	**port block multicast**
Step 4	Block unicast flooding to the port.	**port block unicast**
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries, entering the appropriate command once for the **multicast** option and once for the **unicast** option.	**show port block** {**multicast** | **unicast**} *interface*

For more information on IOS Release 11.2(8)SA6, see the *Cisco IOS Desktop Switching Command Reference.* The complete IOS Release 11.2(8) documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 11.2**.

Reloading and Upgrading the Switch Software

Use the System Configuration page (see Figure 3-11 and Figure 3-12) to specify the Flash memory filenames that the switch uses when it starts or resets. You can also use this page to upgrade your switch firmware.

To display this page, select **System>System Configuration** from the menu bar.

You can use this page for the following tasks:

- Changing the baud rate for the console port.
- Saving the Configuration file and restart the switch.
- Changing the reload options the switch uses when it restarts.
- Upgrading the software running the switch.

Saving the Configuration File

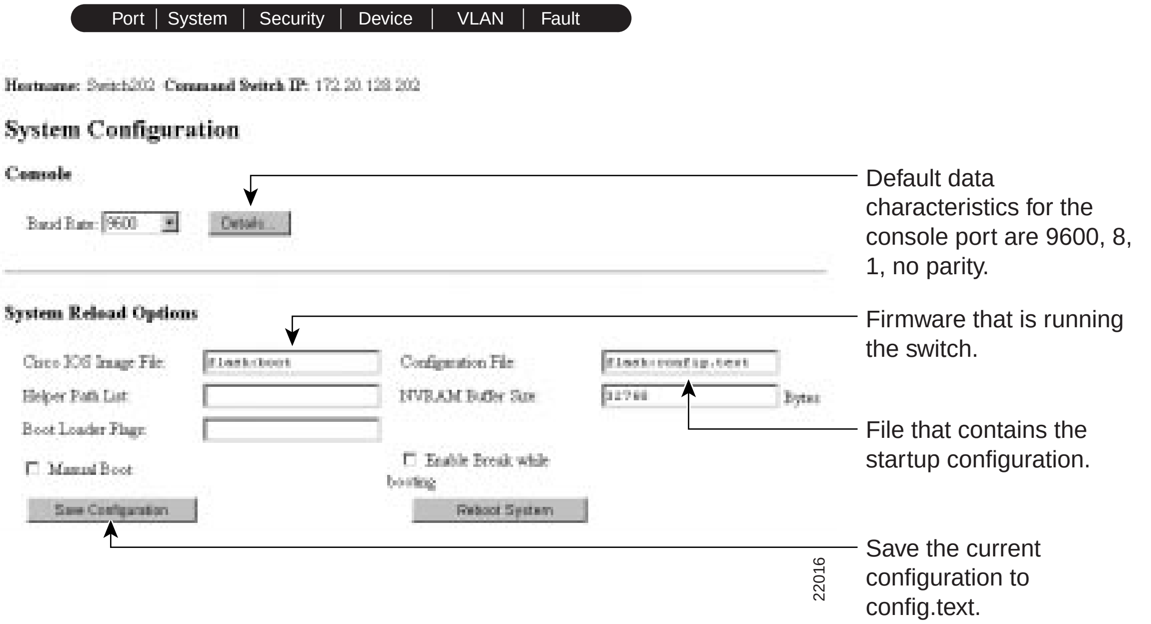
The startup configuration file contains the IP addresses, passwords, and any other information you entered. The switch reloads this file when it restarts. However, the startup configuration file might not be the running (current) configuration. Changes made through the CVSM or the CLI take effect immediately but must be explicitly saved to be included in the startup configuration.

Use this page to save the running configuration to the startup configuration file. The following buttons control the switch startup:

Save Configuration Click to write the running configuration to Flash memory. This configuration is then loaded when the switch is restarted.

Reboot System Click to restart the switch and to load the new startup configuration.

Figure 3-11 System Configuration (Part 1)



Hostname: Switch202 Command Switch IP: 172.20.128.202

System Configuration

Console

Baud Rate: 9600

System Reload Options

Cisco IOS Image File: flash:boot

Configuration File: flash:config.text

Helper Path List:

NVRAM Buffer Size: 32768 Bytes

Boot Loader Flags:

□ Manual Boot

□ Enable Break while booting

Default data characteristics for the console port are 9600, 8, 1, no parity.

Firmware that is running the switch.

File that contains the startup configuration.

Save the current configuration to config.text.

Entering the System Reload Options

By default, the System Reload Options fields contain the correct information to reboot the system. Some of the fields contain files in Flash memory. To determine the filenames to use, enter the following EXEC mode command at the CLI:

```
switch# dir flash:
Directory of flash:

  2  -rwx      843947   Mar 01 1993 00:02:18 C2900XL-hs-mz-112.8-SA6.bin
  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 image file that runs the switch has a .bin extension, the html directory contains the CVSM HTML files, and config.text contains the current configuration. If you need more information about accessing the switch via the CLI, refer to the “Configuring the Switch for Telnet” section on page 2-30.

Click **Help** for procedures on how to configure the fields on this page.

Upgrading Switch Software

When you upgrade a switch or cluster, the switch or switches continue to operate normally while the new software is copied to Flash memory. When the copy is complete, the old files are deleted, and the new software is loaded the next time you reboot. If the browser halts or the copy fails in some way, you can reboot the switch with the old version of the software and re-execute the upgrade procedure.

If you group switches into a cluster, you can upgrade the entire cluster from Cluster Manager. For more information, see the “Upgrading Software for a Group of Switches” section on page 4-16.

New releases of switch software are available on Cisco Connection Online (CCO). The process of upgrading your switch consists of the following steps:

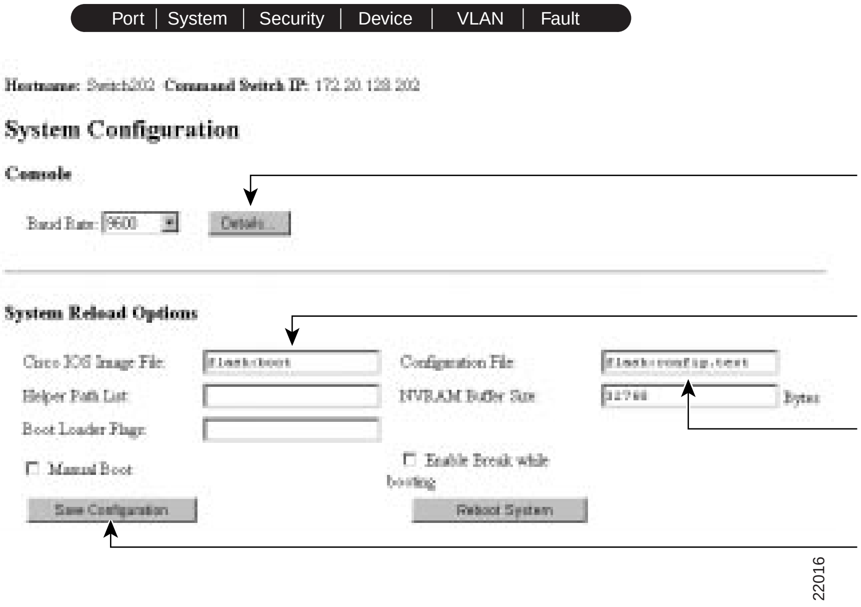
Step 1 Downloading the software from CCO.

Step 2 Downloading a TFTP server if necessary.

Step 3 Entering the name of the new image on this page and clicking **Upgrade Cisco IOS and Visual Switch Manager**.

Click **Help** for the complete procedures for this process.

Figure 3-12 System Configuration (Part 2)



Hostname: Switch202 Command Switch IP: 172.20.128.202

System Configuration

Console

Baud Rate: 9600

System Reload Options

Cisco IOS Image File: flash:boot

Helper Path List:

Boot Loader Flags:

Configuration File: flash:config.text

NVRAM Buffer Size: 32768 Bytes

□ Manual Boot

□ Enable Break while booting

Default data characteristics for the console port are 9600, 8, 1, no parity.

Firmware that is running the switch.

File that contains the startup configuration.

Save the current configuration to config.text.

CLI Commands for Upgrading the Switch Software

This procedure is for switches already running IOS Release 11.2(8)SA6. Switches running earlier IOS releases might have less memory and require slightly different procedures. If you need to upgrade an older switch to this IOS release, refer to the *Release Notes for Cisco IOS Release 11.2(8)SA6* or the release notes that came with your switch.

These steps are included in the upgrade procedure:

- You need to change the name of the *current* image file to the name of the *new* file you are copying. The **tar** command then replaces the old image file with the new one.
- To avoid a conflict with users accessing the CVSM pages during the software upgrade, you need to disable access to the HTML pages and delete the existing HTML files before you upgrade the software.

Follow these steps to upgrade the switch software, starting in privileged EXEC mode:

Task	Command
1 Display the name of the current (default) image file.	switch# **show boot**
2 Rename the current image file to the name of the file that you downloaded, and replace the *tar* extension with *bin*. This step does not affect the operation of the switch.	switch# **rename flash:*current_image* flash:*new_image.bin***
3 Display the contents of Flash memory to verify the renaming of the file.	switch# **dir flash:**
4 Enter global configuration mode.	switch# **configure terminal**
5 Disable access to the switch HTML pages.	switch(config)# **no IP http server**
6 Return to privileged EXEC mode.	switch(config)# **end**
7 Remove the CVSM HTML files.	switch# **delete flash:html/***
8 Use the **tar** command to copy the files into the switch Flash memory. **9** Depending on the TFTP server, you might need to enter only one slash (/) after the *server_ip_address* in the **tar** command.	switch# **tar /x tftp://*server_ip_address*//*path*/*filename*.tar flash:**
10 Enter global configuration mode.	switch# **configure terminal**

Task	Command
11 Reenable access to the switch HTTP pages.	`switch(config)#` **`IP http server`**
12 Return to privileged EXEC mode.	`switch(config)#` **`end`**
13 Reload the new software.	`switch#` **`reload`**

For more information on IOS Release 11.2(8)SA6, see the *Cisco IOS Desktop Switching Command Reference.* The complete IOS Release 11.2(8) documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 11.2**.

Setting the System Date and Time

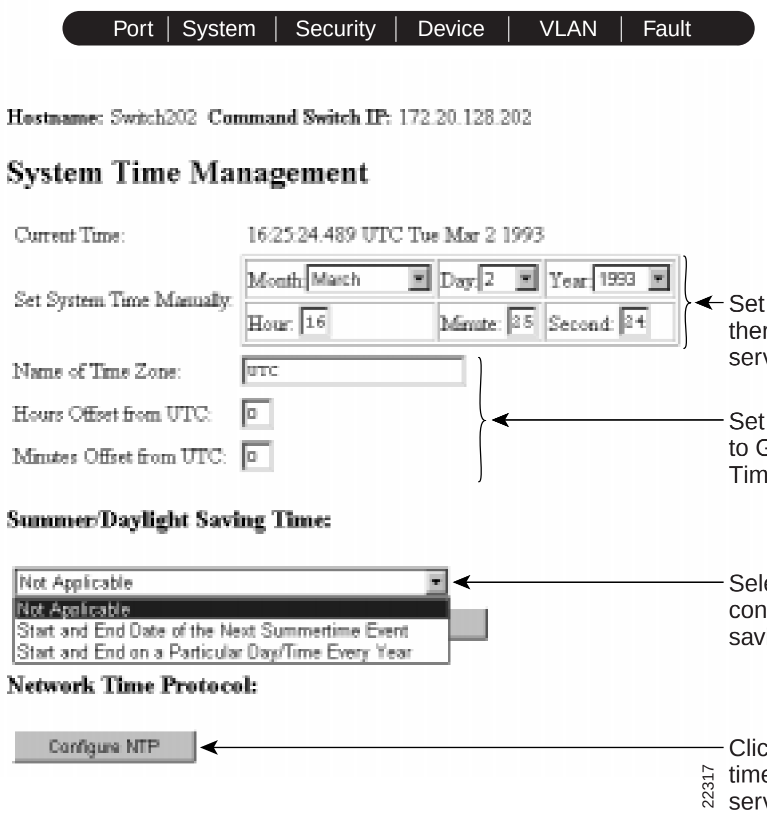
Use the System Time Management page (Figure 3-13) to set the system time for a switch or enable an external source such as Network Time Protocol (NTP) to supply time to the switch.

You can use this page to set the switch time by using one of the following techniques:

- Manually set the system time (including daylight saving time) and date
- Configure the switch to run in NTP client mode and receive time information from an NTP server
- Configure the switch to run in NTP broadcast-client mode and receive information from an NTP broadcast server

To display this page, select **System>System Time Management** from the menu bar.

Figure 3-13 System Time Management



Port
System
Security
Device
VLAN
Fault
Not Applicable
Start and End Date of the Next Summertime Event
Start and End on a Particular Day/Time Every Year
Configure NTP
22317

Hostname: Switch202 **Command Switch IP:** 172.20.128.202

System Time Management

Current Time: 16:25:24.489 UTC Tue Mar 2 1993

Set System Time Manually: Month: March Day: 2 Year: 1993 Hour: 16 Minute: 25 Second: 24

Name of Time Zone: UTC

Hours Offset from UTC: 0

Minutes Offset from UTC: 0

Summer/Daylight Saving Time:

Not Applicable

Network Time Protocol:

Set time manually if there is no NTP server.

Set time in relation to Greenwich Mean Time.

Select item to configure daylight saving time.

Click to configure time from a NTP server.

Setting the System Date and Time

Enter the date and a 24-hour clock time setting on the System Time Management page. If you are entering the time for an American time zone, enter the three-letter abbreviation for the time zone in the **Name of Time Zone** field. If you are identifying the time zone by referring to Greenwich Mean Time, enter UTC (Universal Time Coordinated) in the **Name of Time Zone** field. You then must enter a negative or positive number as an offset to indicate the number of time zones the switch is from Greenwich, England. Enter a negative number if the switch is west of Greenwich, England, and east of the International Date Line. California is eight time zones west of Greenwich, and you would enter -8 in the **Hours Offset From UTC** field. Negative and positive numbers can also be entered for minutes.

To configure daylight saving time, select an option from the drop-down menu, and Click **Configure Summer/Daylight Saving Time**. You can configure the switch to change to daylight saving time on a particular day every year, on a day that you enter, or not at all.

Configuring the Network Time Protocol

In complex networks it can make sense to distribute time information from a central server. The NTP can distribute time information by responding to requests from clients or by broadcasting time information. You can use the Network Time Protocol page (Figure 3-14) to enable these options and to enter authentication information to accompany NTP client requests.

To display this page, click **Configure NTP** on the System Time Management page.

Configuring the Switch as an NTP Client

You configure the switch as an NTP client by entering the IP addresses of up to ten NTP servers in the **IP Addr** field. Click **Preferred** to specify which server should be used first. You can also enter an authentication key to be used as a password when requests for time information are sent to the server.

Enabling NTP Authentication

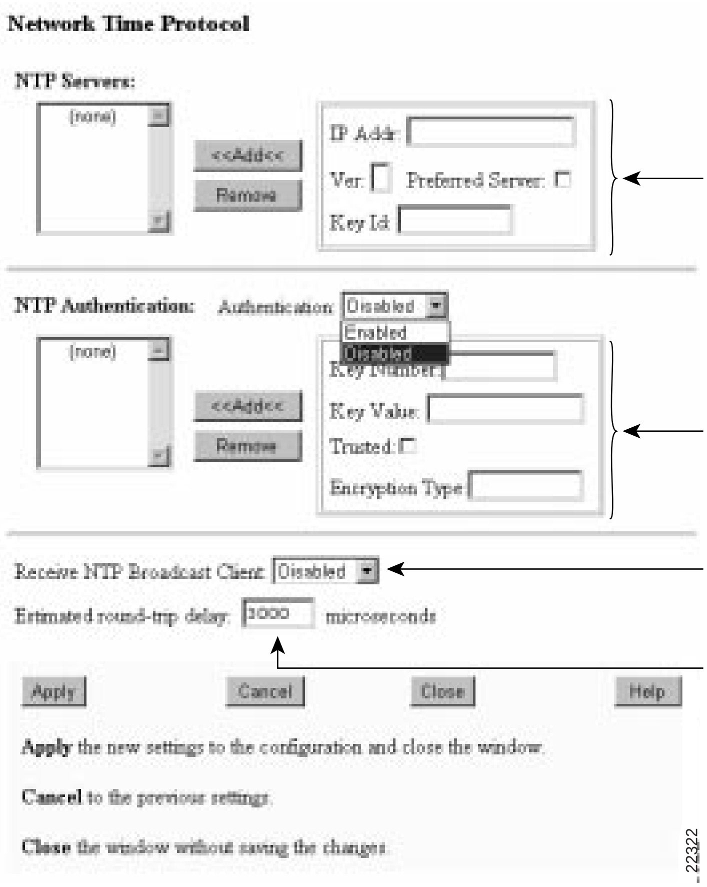
To ensure the validity of information received from NTP servers, you can authenticate NTP messages with public-key encryption. This procedure must be coordinated with the administrator of the NTP servers: the information you enter on this page will be matched by the servers to authenticate it.

Click **Help** for more information about entering information in the **Key Number**, **Key Value**, and **Encryption Type** fields.

Configuring the Switch for NTP Broadcast-Client Mode

You can configure the switch to receive NTP broadcast messages if there is an NTP broadcast server, such as a router, broadcasting time information on the network. You can also enter a delay in the **Estimated Round-Trip Delay** field to account for round-trip delay between the client and the NTP broadcast server.

Figure 3-14 Network Time Protocol



Network Time Protocol

NTP Servers: (none)

IP Addr:

Ver: □ Preferred Server: □

Key Id:

NTP Authentication: Authentication: Disabled (Enabled / Disabled)

(none)

Key Number:

Key Value:

Trusted: □

Encryption Type:

Receive NTP Broadcast Client: Disabled

Estimated round-trip delay: 3000 microseconds

Apply the new settings to the configuration and close the window.

Cancel to the previous settings.

Close the window without saving the changes.

Configure the NTP server for the switch. Key ID is for authentication.

Enable NTP authentication.

Enable the switch to receive NTP broadcast packets.

Enter a delay in microseconds to allow for the estimated broadcast interval.

Configuring IP Information

Use the IP Management page (see Figure 3-15) to change or enter IP information for the switch. Some of this information, such as the IP address, you had previously entered.

To change IP information for the switch, select **System>IP Management** from the menu bar.

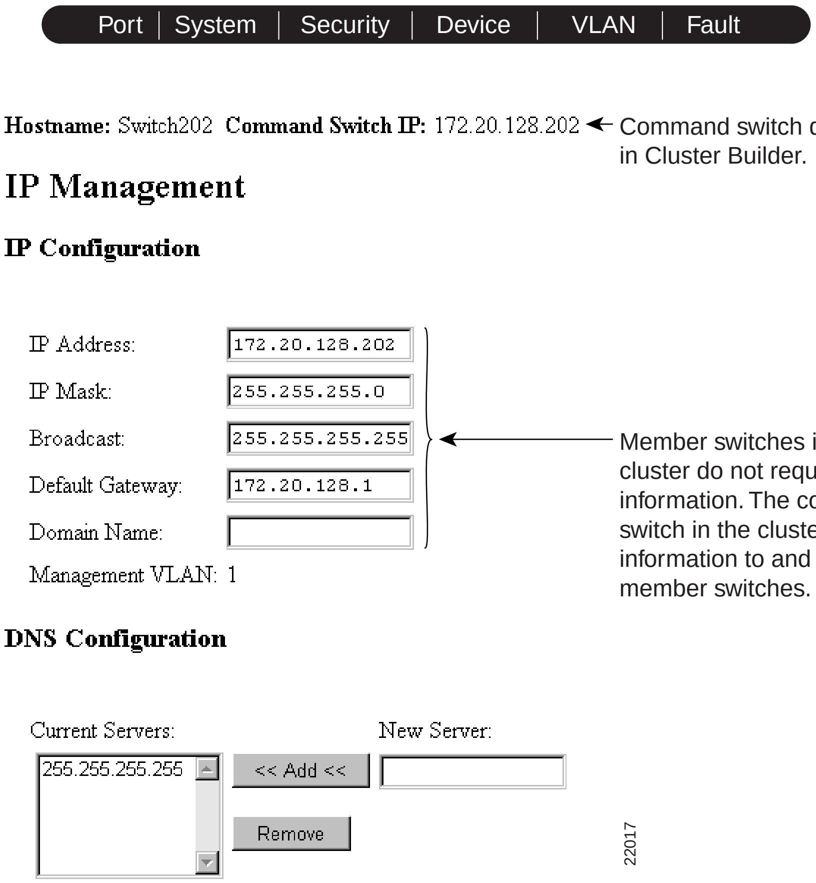
Configuring the Switch for IP

The switch IP address belongs to VLAN 1 and is used to access interfaces such as the CVSM and SNMP. For a port to access one of these management interfaces, it must also belong to VLAN 1.

If your switch is configured as a member switch in a cluster, it might not have an IP address assigned to it. If your switch is configured as a command switch in a cluster, its IP information supports the IP connectivity of all its member switches.

Caution Changing the switch IP address on this page ends your CVSM session. Restart the CVSM by entering the new IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer), as described in the "Using Cisco Visual Switch Manager" section on page 2-6.

Figure 3-15 IP Management



Hostname: Switch202 **Command Switch IP:** 172.20.128.202

Command switch defined in Cluster Builder.

IP Management

IP Configuration

IP Address:	172.20.128.202
IP Mask:	255.255.255.0
Broadcast:	255.255.255.255
Default Gateway:	172.20.128.1
Domain Name:	
Management VLAN:	1

Member switches in a cluster do not require IP information. The command switch in the cluster directs information to and from the member switches.

DNS Configuration

Current Servers: 255.255.255.255

New Server:

CLI Commands for Assigning IP Information to the Switch

Beginning in privileged EXEC mode, follow these steps to enter the IP information:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port to which the IP information is assigned. VLAN 1 is the switch interface.	**interface vlan 1**
Step 3	Enter the IP address and subnet mask.	**ip address** *ip_address subnet_mask*
Step 4	Enter the IP address of the default router.	**ip default-gateway** *ip_address*
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify that the information was entered correctly by displaying the running configuration. If the information is incorrect, repeat the procedure.	**show running-config**

For more information on IOS Release 11.2(8)SA6, see the *Cisco IOS Desktop Switching Command Reference.* The complete IOS Release 11.2(8) documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 11.2**.

Configuring SNMP

Use the SNMP Configuration page (Figure 3-16) to configure your switch for SNMP management.

To display this page, select **System>SNMP Configuration** from the menu bar.

This guide describes the use of IOS commands that have been created or changed for use with switches that support IOS Release 11.2(8)SA6. For information on other IOS Release 11.2(8) commands, see the IOS documentation set available from the CCO home page by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 11.2**.

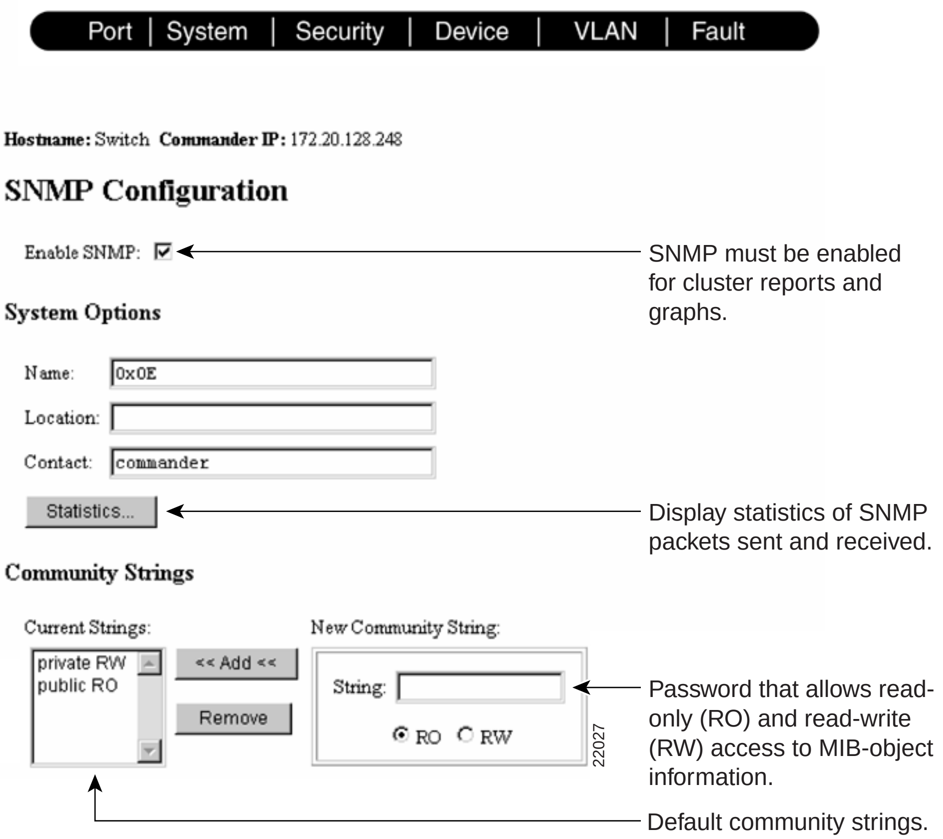
Use this page to perform the following tasks:

- Disable and enable SNMP.
- Enter information about the switch (System Options).
- Enter community strings that serve as passwords for SNMP messages.
- Enter trap managers and their community strings to receive traps (alerts) about switch activity.
- Set the classes of traps a trap manager receives.
- Display statistics.

Disabling and Enabling SNMP

If you deselect **Enable SNMP** and click **Apply**, SNMP is disabled, and the SNMP parameters on the page disappear. SNMP must be enabled for some network view and Cluster Management features to work properly. For information SNMP and Cluster Management, see “Managing Clusters via SNMP” section on page 2-35.

Figure 3-16 SNMP Configuration - Part 1



Hostname: Switch **Commander IP:** 172.20.128.248

SNMP Configuration

Enable SNMP: ☑

System Options

Name: 0x0E

Location:

Contact: commander

Community Strings

Current Strings: private RW, public RO

New Community String:

String:

● RO ○ RW

SNMP must be enabled for cluster reports and graphs.

Display statistics of SNMP packets sent and received.

Password that allows read-only (RO) and read-write (RW) access to MIB-object information.

Default community strings.

Entering Community Strings

Community strings serve as passwords for SNMP messages. You can enter them with the following characteristics:

Read only (RO) Requests accompanied by the string can display MIB-object information.

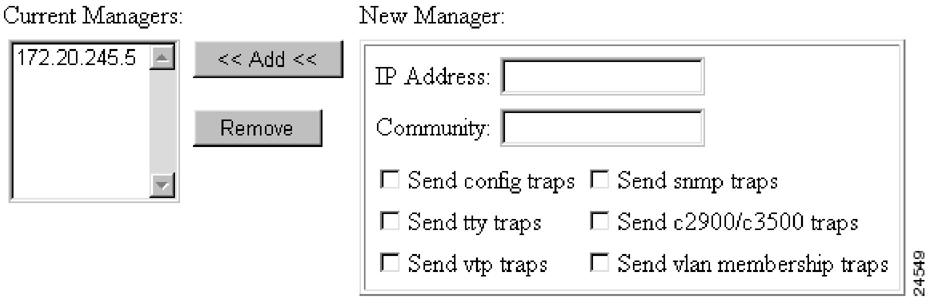
Read write (RW) Requests accompanied by the string can display MIB-object information and set MIB objects.

Adding Trap Managers

A trap manager is a management station that receives and processes traps. When you configure a trap manager, community strings for each member switch must be unique. If a member switch has an IP address assigned to it, the management station accesses the switch via the IP address.

By default, no trap manager is defined, and no traps are issued.

Figure 3-17 SNMP Configuration - Part 2



Current Managers: 172.20.245.5

IP Address:

Community:

☐ Send config traps ☐ Send snmp traps

☐ Send tty traps ☐ Send c2900/c3500 traps

☐ Send vtp traps ☐ Send vlan membership traps

Select a check box to enable on of the following classes of traps:

Send config traps	Generate traps whenever the switch configuration changes.
Send SNMP traps	Generate the supported SNMP traps.
Send TTY traps	Generate traps when the switch starts a management console CLI session.
Send C2900, C3500 traps	Generate the switch-specific traps. These traps are in the private enterprise-specific MIB.
Send VTP traps	Generate a trap for each VLAN Trunk Protocol (VTP) change (Enterprise Edition Software only).
Send VLAN membership traps	Generate a trap for each VLAN Membership Policy Server (VMPS) change (Enterprise Edition Software only).

CLI Commands for Adding a Trap Manager

Beginning in privileged EXEC mode, follow these steps to add a trap manager and community string:

Task		Command
Step 1	Enter global configuration mode.	**config terminal**
Step 2	Enter the trap manager IP address, community string, and the traps to generate.	**snmp-server host 172.2.128.263 traps1 snmp vlan-membership**
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify that the information was entered correctly by displaying the running configuration.	**show running-config**

For more information on IOS Release 11.2(8)SA6, see the *Cisco IOS Desktop Switching Command Reference.* The complete IOS Release 11.2(8) documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 11.2**.

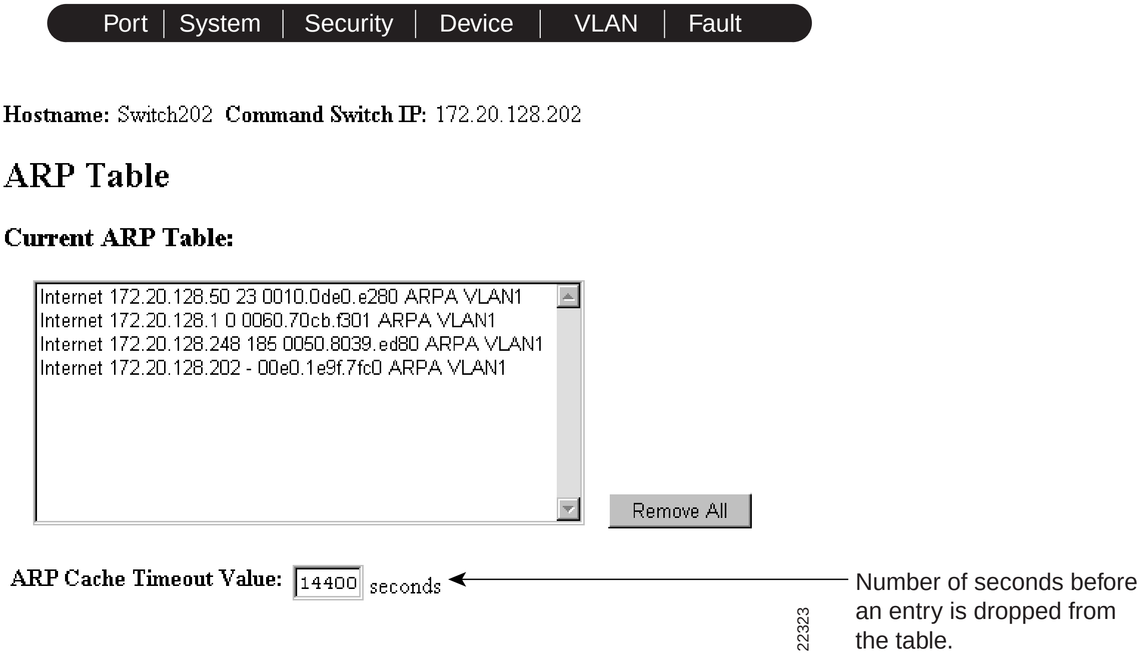
Managing the ARP Table

Use the ARP Table page (Figure 3-18) to display the table and change the timeout value. The Address Resolution Protocol (ARP) discovers the MAC address and VLAN ID that corresponds to a host IP address. Figure 3-19 shows the meaning the of ARP table contents.

To display this page, select **System>ARP Table** from the menu bar. ARP entries added manually to the table do not age and must be manually removed.

This guide describes the use of IOS commands that have been created or changed for use with switches that support IOS Release 11.2(8)SA6. For information on other IOS Release 11.2(8) commands, see the IOS documentation set available from the CCO home page by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 11.2**.

Figure 3-18 ARP Table


Port
System
Security
Device
VLAN
Fault
Remove All
Number of seconds before an entry is dropped from the table.
22323

Hostname: Switch202 **Command Switch IP:** 172.20.128.202

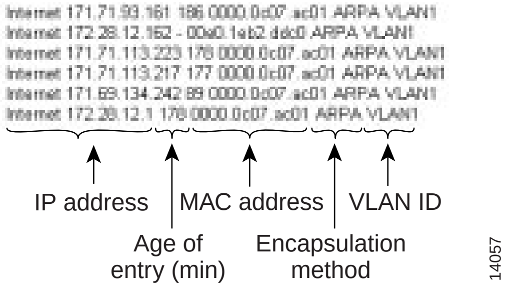
ARP Table

Current ARP Table:

```
Internet 172.20.128.50 23 0010.0de0.e280 ARPA VLAN1
Internet 172.20.128.1 0 0060.70cb.f301 ARPA VLAN1
Internet 172.20.128.248 185 0050.8039.ed80 ARPA VLAN1
Internet 172.20.128.202 - 00e0.1e9f.7fc0 ARPA VLAN1
```

ARP Cache Timeout Value: 14400 seconds

Figure 3-19 Contents of the ARP Table



```
Internet 171.71.93.161 186 0000.0c07.ac01 ARPA VLAN1
Internet 172.28.12.162 - 00e0.1eb2.ddc0 ARPA VLAN1
Internet 171.71.113.223 178 0000.0c07.ac01 ARPA VLAN1
Internet 171.71.113.217 177 0000.0c07.ac01 ARPA VLAN1
Internet 171.69.134.242 89 0000.0c07.ac01 ARPA VLAN1
Internet 172.28.12.1 178 0000.0c07.ac01 ARPA VLAN1
```

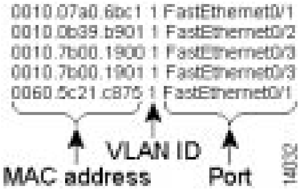
Managing the MAC Address Tables

Use the Address Management page (see Figure 3-21) to manage the MAC address tables that the switch uses to forward traffic between ports. These MAC tables include the dynamic, secure, and static addresses.

To display this page, select **Security>Address Management** from the menu bar.

The address tables list the destination MAC address and the associated VLAN ID, module, and port number associated with the address. Figure 3-20 shows a list of dynamic addresses.

Figure 3-20 Contents of the Address Table



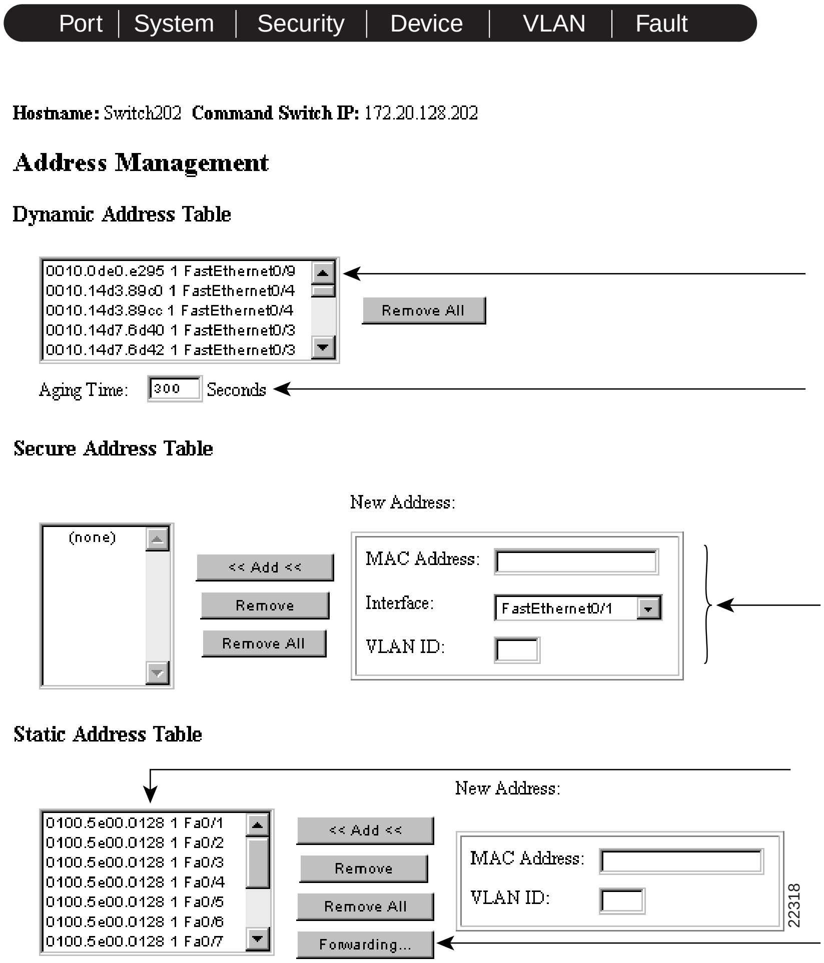
```
0010.07a0.6bc1 1 FastEthernet0/1
0010.0b39.b901 1 FastEthernet0/2
0010.7b00.1900 1 FastEthernet0/3
0010.7b00.1901 1 FastEthernet0/3
0060.5c21.c876 1 FastEthernet0/1
```

MAC Addresses and VLANs

All addresses are associated with a VLAN. An address can exist in more than one VLAN and have different destinations in each. Multicast addresses, for example, could be forwarded to port 1 in VLAN 1 and ports 9, 10, and 11 in VLAN 5. A known address in one VLAN is unknown in another until it is learned or statically associated with a port in the other VLAN.

An address can be secure in one VLAN and dynamic in another. Addresses that are statically entered in one VLAN must be static addresses in all other VLANs. Each VLAN maintains its own logical address table.

Figure 3-21 Address Management



Hostname: Switch202 **Command Switch IP:** 172.20.128.202

Address Management

Dynamic Address Table

```
0010.0de0.e295 1 FastEthernet0/9
0010.14d3.89c0 1 FastEthernet0/4
0010.14d3.89cc 1 FastEthernet0/4
0010.14d7.6d40 1 FastEthernet0/3
0010.14d7.6d42 1 FastEthernet0/3
```

Aging Time: 300 Seconds

Secure Address Table

(none)

New Address:

MAC Address:

Interface: FastEthernet0/1

VLAN ID:

Static Address Table

```
0100.5e00.0128 1 Fa0/1
0100.5e00.0128 1 Fa0/2
0100.5e00.0128 1 Fa0/3
0100.5e00.0128 1 Fa0/4
0100.5e00.0128 1 Fa0/5
0100.5e00.0128 1 Fa0/6
0100.5e00.0128 1 Fa0/7
```

New Address:

MAC Address:

VLAN ID:

MAC addresses learned by the switch.

Number of seconds before an address is dropped from the table.

Enter a secure MAC address for a port. Secure the port on the Port Security page.

MAC addresses entered manually do not age and are not lost when the switch resets.

Click to define the forwarding behavior of the MAC address.

Changing the Address Aging Time

Dynamic addresses are source MAC addresses that the switch learns and then drops when they are not in use. Use the Aging Time field to define how long the switch retains unseen addresses in the table. This parameter applies to all VLANs.

CLI Commands to Define the Aging Time

Beginning in privileged EXEC mode, follow these steps to define the aging time for the address table.

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter the number of seconds that dynamic addresses are to be retained in the address table. You can enter a number from 10 to 1000000.	**mac-address-table aging-time** *seconds*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show mac-address-table aging-time**

Adding Secure Addresses

The secure address table contains secure MAC addresses and their associated ports and VLANs. A secure address is a manually entered unicast address that is forwarded to only one port per VLAN. If you enter an address that is already assigned to another port, the switch reassigns the secure address to the new port. Secure addresses do not age and can be either manually entered into the address table or learned.

You can enter a secure port address even when the port does not yet belong to the VLAN. When the port is later assigned to the VLAN, packets destined for that address are forwarded to the port.

To display this page, select **Security>Address Management** from the menu bar.

After you have entered the secure address, select **Security>Port Security** from the menu bar to secure the port on the Port Security page.

CLI Commands for Adding Secure Addresses

Beginning in privileged EXEC mode, follow these steps to enter a secure address:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter the MAC address, its associated port, and the VLAN ID.	**mac-address-table secure** *hw-addr interface* **vlan** *vlan-id*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show mac-address-table secure**

Adding and Removing Static Addresses

A static address has the following characteristics:

- It is manually entered in the address table and must be manually removed.
- It can be a unicast or multicast address.
- It does not age and is retained when the switch restarts.

The Static Address Forwarding map (Figure 3-22) displays when you enter a static address. Use this page to define those ports that frames are forwarded to based on the port on which they were received. Because all ports are associated with at least one VLAN, the switch acquires the VLAN ID for the address from the ports that you select on the forwarding map.

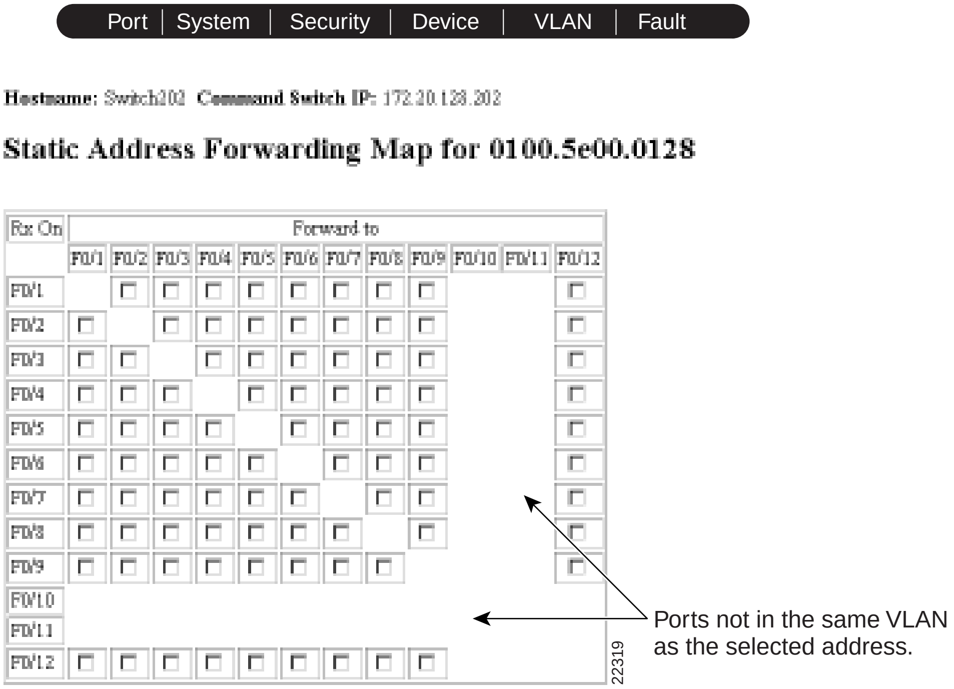
The Rx On column on the left lists the source ports. The Forward to columns across the page are the destination ports. Ports without check boxes belong to VLANs that a source port cannot access.

A static address in one VLAN must be a static address in other VLANs. A packet with a static address that arrives on a VLAN where it has not been statically entered is flooded to all ports and not learned.

To display this page, select **Security>Address Management** from the menu bar, and enter or select an address in the Static Address Table.

Note If you want to forward to a port for which there is no check box, add that port to a VLAN to which the forwarding port belongs.

Figure 3-22 Static Address Forwarding Map



Hostname: Switch202 **Command Switch IP:** 172.20.128.202

Static Address Forwarding Map for 0100.5e00.0128

Rx On	Forward to											
	F0/1	F0/2	F0/3	F0/4	F0/5	F0/6	F0/7	F0/8	F0/9	F0/10	F0/11	F0/12
F0/1		□	□	□	□	□	□	□	□			□
F0/2	□		□	□	□	□	□	□	□			□
F0/3	□	□		□	□	□	□	□	□			□
F0/4	□	□	□		□	□	□	□	□			□
F0/5	□	□	□	□		□	□	□	□			□
F0/6	□	□	□	□	□		□	□	□			□
F0/7	□	□	□	□	□	□		□	□			□
F0/8	□	□	□	□	□	□	□		□			□
F0/9	□	□	□	□	□	□	□	□				□
F0/10												
F0/11												
F0/12	□	□	□	□	□	□	□	□	□			

Ports not in the same VLAN as the selected address.

Configuring Static Addresses for EtherChannel Port Groups

Follow these rules if you are configuring a static address to forward to ports in an EtherChannel port group:

- For default source-based port groups, configure the static address to forward to *all ports* in the port group to eliminate lost packets.
- For destination-based port groups, configure the address to forward to *only one port* in the port group to avoid the transmission of duplicate packets.

CLI Commands for Adding Static Addresses

Static addresses are entered in the address table with an *in-port-list* and an *out-port-list* and, as needed, a VLAN definition. Packets received from the in-port are forwarded to ports listed in the out-port-list.

Note If the in-port and out-port-list parameters are all access ports in a single VLAN, you can omit the VLAN identification. In this case, the switch recognizes the VLAN as that associated with the in-port VLAN. Otherwise, you must supply the VLAN ID.

Beginning in privileged EXEC mode, follow these steps to enter a static address:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter the MAC address, the input port, the ports to which it can be forwarded, and the VLAN ID of those ports.	**mac-address-table static** *hw-addr in-port out-port-list* **vlan** *vlan-id*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show mac-address-table static**

For more information on IOS Release 11.2(8)SA6, see the *Cisco IOS Desktop Switching Command Reference.* The complete IOS Release 11.2(8) documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 11.2Cisco IOS Release 11.2**.

Enabling Port Security

Use the Port Security page (Figure 3-23) to enable port security and to define the size of the secured port address table.

To display this page, select **Security>Port Security** from the menu bar.

Secured ports restrict the use of a port to a user-defined group of stations. When you assign secure addresses to a secure port, the switch does not forward any packets with source addresses outside the group. If you define the address table of a secure port to contain only one address, the workstation or server attached to that port is guaranteed the full bandwidth of the port.

Secured ports generate address-security violations under the following conditions:

- The address table of a secured port is full and the address of an incoming packet is not found in the table.
- An incoming packet has a source address assigned as a secure address on another port.

Limiting the number of devices that can connect to a secure port has the following advantages:

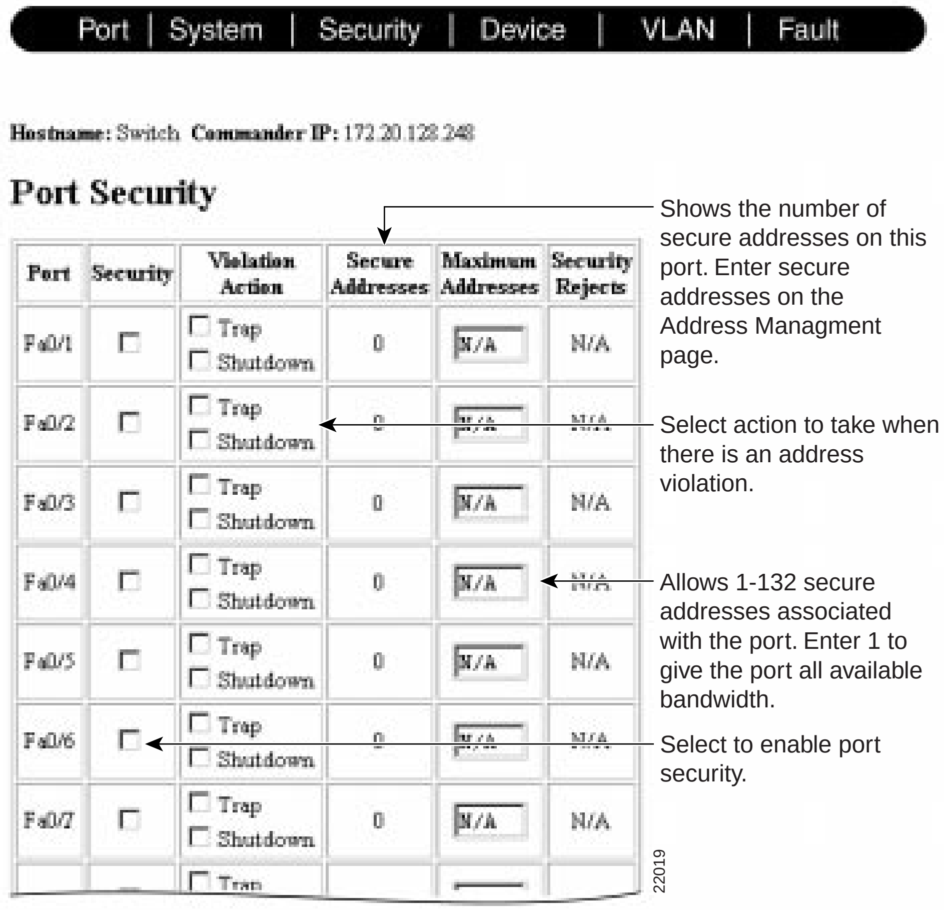
- Dedicated bandwidth—If the size of the address table is set to 1, the attached device is guaranteed the full bandwidth of the port.
- Added security—Unknown devices cannot connect to the port.

The following fields validate port security or indicate security violations:

Secure Addresses	The number of addresses in the address table for this port. Secure ports have at least one in this field.
Security Rejects	The number of unauthorized addresses seen on the port.

The port features that are unavailable to secure ports are described in the "Preparing to Use the Web-Based Management Interfaces" section on page 2-2.

Figure 3-23 Port Security



Hostname: Switch **Commander IP:** 172.20.128.248

Port Security

Port	Security	Violation Action	Secure Addresses	Maximum Addresses	Security Rejects
Fa0/1	□	□ Trap □ Shutdown	0	N/A	N/A
Fa0/2	□	□ Trap □ Shutdown	0	N/A	N/A
Fa0/3	□	□ Trap □ Shutdown	0	N/A	N/A
Fa0/4	□	□ Trap □ Shutdown	0	N/A	N/A
Fa0/5	□	□ Trap □ Shutdown	0	N/A	N/A
Fa0/6	□	□ Trap □ Shutdown	0	N/A	N/A
Fa0/7	□	□ Trap □ Shutdown	0	N/A	N/A
		□ Trap			

Shows the number of secure addresses on this port. Enter secure addresses on the Address Managment page.

Select action to take when there is an address violation.

Allows 1-132 secure addresses associated with the port. Enter 1 to give the port all available bandwidth.

Select to enable port security.

Defining the Maximum Secure Address Count

A secure port can have from 1 to 132 associated secure addresses. Setting the MAC address table associated with the port to have one address ensures the attached device has the full bandwidth of the port.

CLI Commands to Enable Port Security

The following example shows the commands for enabling port security and setting the port to learn only one address. This procedure disables the port if a security violation occurs. Starting in privileged EXEC mode, follow these steps to enable port security.

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode for the port you want to secure.	**interface** *interface*
Step 3	Secure the port and set the address table to one address.	**port security max-mac-count 1**
Step 4	Set the port to shutdown when a security violation occurs.	**port security shutdown**
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify the entry.	**show port security**

For more information on IOS Release 11.2(8)SA6, see the *Cisco IOS Desktop Switching Command Reference.* The complete IOS Release 11.2(8) documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 11.2**.

Configuring the Cisco Discovery Protocol

Use the Cisco Discovery Protocol (CDP) page to enable CDP for the switch, set global CDP parameters, and display information about neighboring Cisco devices. CDP enables CVSM and other network management applications to display a graphical network view of the network. For example, the switch uses CDP to find cluster candidates and maintain information about cluster members and other devices. The information exchanged in CDP messages includes the device type, links between devices, and the number of ports within each device. Based on the CDP messages sent, the switch displays these devices in the network view and the Cluster Manager.

Note Creating and maintaining switch clusters is based on the regular exchanging of CDP messages. Turning off CDP can interrupt cluster discovery. If you are changing cables between switches often, you can improve the cluster-discovery performance by lowering the value in the **Packets sent every** field.

To display this page (see Figure 3-24), select **Device>Cisco Discovery Protocol** from the menu bar.

Configuring CDP

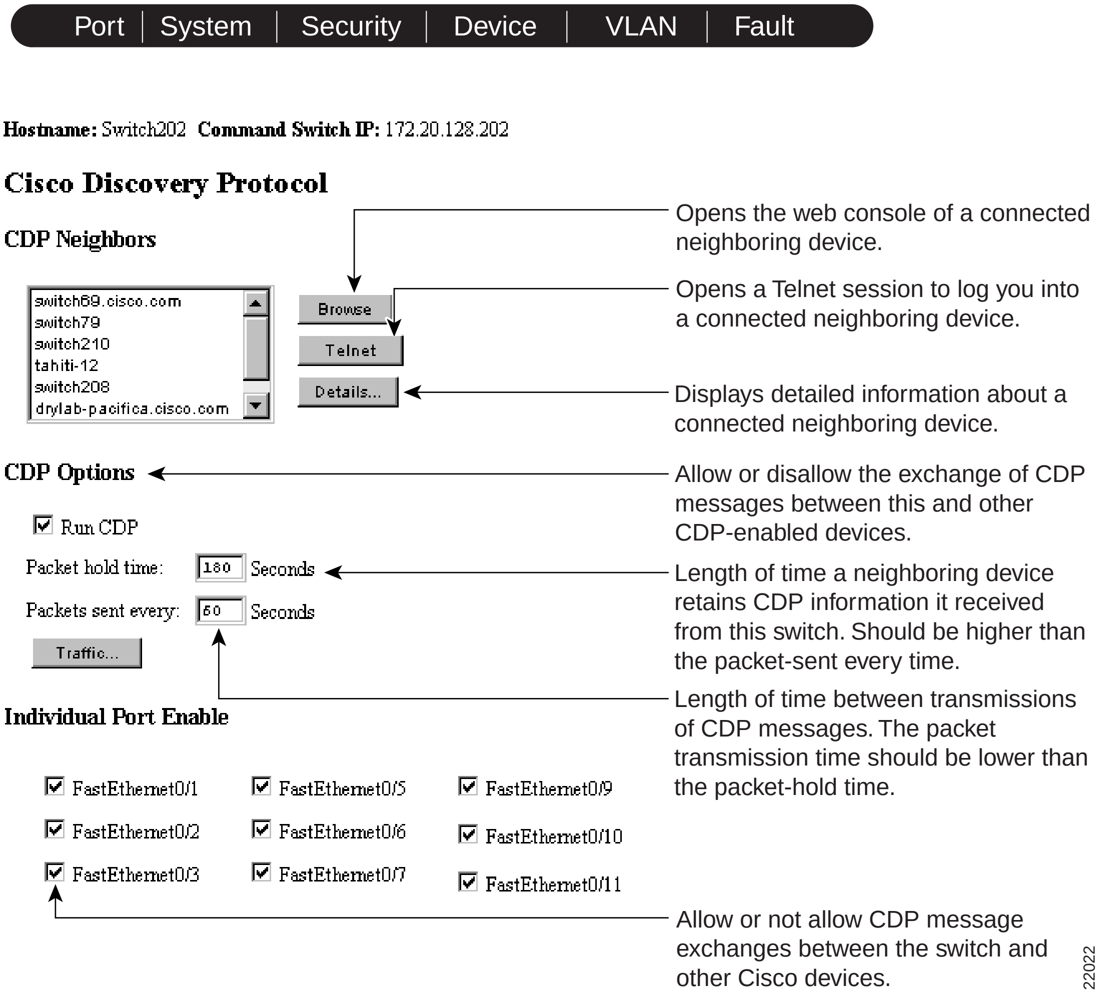
Some CDP options are global to the switch, and some are entered on a per-port basis. CDP is enabled by default. Click **Help** for the defaults and possible values of the fields on this page. You can use this page for the following tasks:

- Listing and displaying neighboring devices. The CDP Neighbors list shows the devices with which this switch is exchanging CDP messages. Depending on the management interfaces supported on the neighboring device, you can access it via Telnet or through an HTML interface, and you can display the most recent information received from the device.
- Setting CDP Options. When you deselect the Run CDP checkbox, you disable CDP for the entire switch and changes in the Individual Port Enable section have no effect.
- Disabling CDP on individual ports

CLI Commands for Configuring CDP

This guide describes the use of IOS commands that have been created or changed for use with switches that support IOS Release 11.2(8)SA6. For information on other IOS Release 11.2(8) commands, see the IOS documentation set available from the CCO home page by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 11.2**.

Figure 3-24 Cisco Discovery Protocol



Hostname: Switch202 **Command Switch IP:** 172.20.128.202

Cisco Discovery Protocol

CDP Neighbors

switch69.cisco.com
switch79
switch210
tahiti-12
switch208
drylab-pacifica.cisco.com

CDP Options

☑ Run CDP

Packet hold time: 180 Seconds

Packets sent every: 60 Seconds

Individual Port Enable

☑ FastEthernet0/1 ☑ FastEthernet0/5 ☑ FastEthernet0/9
☑ FastEthernet0/2 ☑ FastEthernet0/6 ☑ FastEthernet0/10
☑ FastEthernet0/3 ☑ FastEthernet0/7 ☑ FastEthernet0/11

Opens the web console of a connected neighboring device.

Opens a Telnet session to log you into a connected neighboring device.

Displays detailed information about a connected neighboring device.

Allow or disallow the exchange of CDP messages between this and other CDP-enabled devices.

Length of time a neighboring device retains CDP information it received from this switch. Should be higher than the packet-sent every time.

Length of time between transmissions of CDP messages. The packet transmission time should be lower than the packet-hold time.

Allow or not allow CDP message exchanges between the switch and other Cisco devices.

Controlling IP Management Packets via CGMP

Use the Cisco Group Management Protocol page (see Figure 3-25) to enable Cisco Group Management Protocol (CGMP) and the CGMP Fast Leave option. CGMP reduces the unnecessary flooding of IP multicast packets by limiting the transmission of these packets to CGMP clients that request them. The Fast Leave option accelerates the removal of unused CGMP groups. By default, CGMP is enabled, and the Fast Leave option is disabled.

To display this page, select **Device>Cisco Group Management Protocol** from the menu bar.

End stations issue join messages to become part of a CGMP group and issue leave messages to leave the group. The membership of these groups is managed by the switch and connected routers through the further exchange of CGMP messages.

CGMP groups are maintained by VLAN: a multicast IP address packet can be forwarded to one list of ports in one VLAN and to a different list of ports in another VLAN. When a CGMP group is added or removed, all members are in the same VLAN.

You can use this page to perform the following tasks:

- Disable CGMP
- Enable the Fast Leave option
- Manually list and remove multicast groups

Enabling Fast Leave Option

The CGMP Fast Leave option reduces the delay when group members leave groups. When an end station requests to leave a CGMP group, the group remains enabled for that VLAN until all members have requested to leave. With the Fast Leave option enabled, the switch immediately checks if there are other members that belong to that group. If there are no other members, the switch removes the port from the group. If there are no other ports in the group, the switch sends a message to routers connected to the VLAN to delete the entire group.

CLI Commands for Enabling the CGMP Fast Leave Option

CGMP reduces flooding by limiting the forwarding of IP multicast and broadcast packets. The Fast Leave option reduces the time CGMP uses to remove inactive groups.

Beginning in privileged EXEC mode, complete these tasks to enable CGMP Fast Leave option:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable CGMP and CGMP Fast Leave.	**cgmp leave-processing**
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show running-config**

Modifying the Router Hold Time

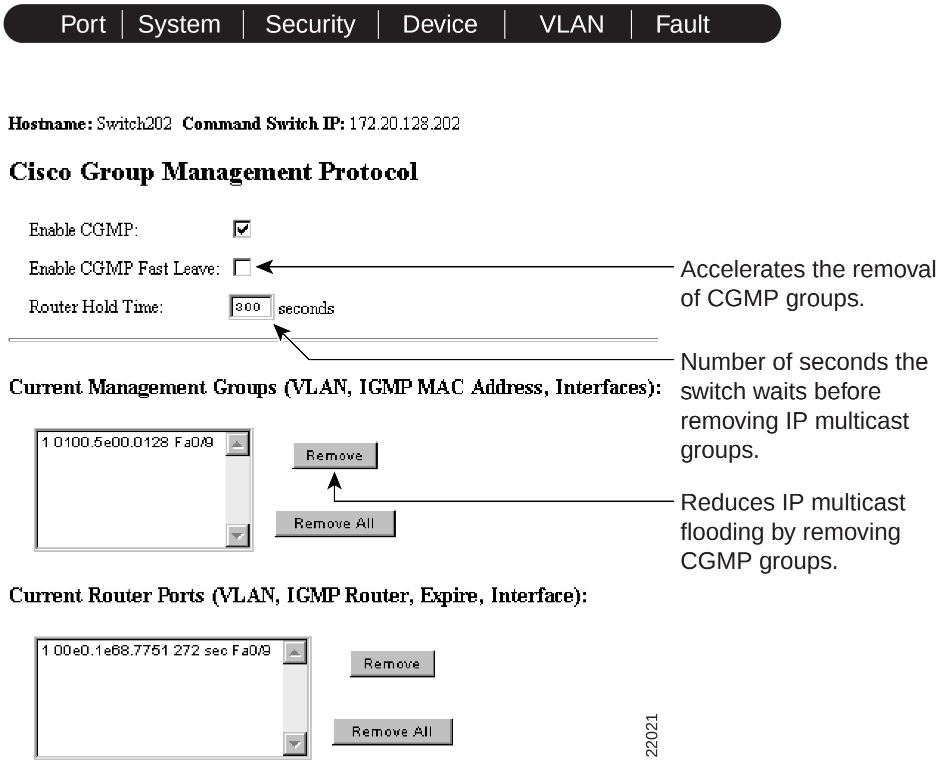
The router hold time is the number of seconds the switch waits before removing (aging) a router entry and ceasing to exchange messages with it. If it is the last router entry on a VLAN, then all groups on that VLAN are removed. You can thus enter a lower number in the Router Hold Time field to accelerate the removal of CGMP groups.

CLI Commands for Changing the Router Hold Time

Beginning in privileged EXEC mode, follow these steps to change the router hold time.

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Configure the number of seconds the switch is to wait before dropping a router entry.	**cgmp holdtime 400**
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show running-config**

Figure 3-25 Cisco Group Management Protocol



Hostname: Switch202 **Command Switch IP:** 172.20.128.202

Cisco Group Management Protocol

Enable CGMP: ☑

Enable CGMP Fast Leave: □

Router Hold Time: 300 seconds

Current Management Groups (VLAN, IGMP MAC Address, Interfaces):

1 0100.5e00.0128 Fa0/9

Current Router Ports (VLAN, IGMP Router, Expire, Interface):

1 00e0.1e68.7751 272 sec Fa0/9

Accelerates the removal of CGMP groups.

Number of seconds the switch waits before removing IP multicast groups.

Reduces IP multicast flooding by removing CGMP groups.

Removing Multicast Groups

You can reduce the forwarding of IP multicast packets by removing groups from the Current Multicast Groups table. Each entry in the table consists of the VLAN, IGMP multicast address, and ports.

CLI Commands for Removing Multicast Groups

You can use the CLI to clear all CGMP groups, all CGMP groups in a VLAN, or all routers, their ports, and their expiration times. Beginning in privileged EXEC mode, follow these steps to remove all multicast groups.

Task		Command
Step 1	Clear all CGMP groups on the switch.	**clear cgmp group**
Step 2	Verify your entry by displaying CGMP information.	**show cgmp**

For more information on IOS Release 11.2(8)SA6, see the *Cisco IOS Desktop Switching Command Reference.* The complete IOS Release 11.2(8) documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 11.2**.

Configuring Spanning-Tree Protocol

Use the Spanning-Tree Protocol (STP) page (Figure 3-26) to change parameters for STP, an industry standard for avoiding loops in switched networks. The switch supports up to 64 instances of STP.

To display this page, select **Device>Spanning-Tree Protocol** from the menu bar.

Because each VLAN has its own instance of STP, you must first select a VLAN ID, and then click **Modify STP Parameters** to display the rest of the page.

This page is shown in three illustrations. Figure 3-26 shows the page with no parameters; Figure 3-27 shows the parameters currently used by the switch and the parameters that this switch would use if it became the root switch. Figure 3-28 shows the fields that you use to define port-level parameters.

Using STP to Support Redundant Connectivity

You can create a redundant backbone with STP by connecting two of the switch ports to another device or to two different devices. STP automatically disables one port, but enables it if the other port is lost. If one link is high-speed and the other low-speed, the low-speed link is always disabled. If the speed of the two links is the same, the port priority and port ID are added together, and STP disables the link with the lowest value.

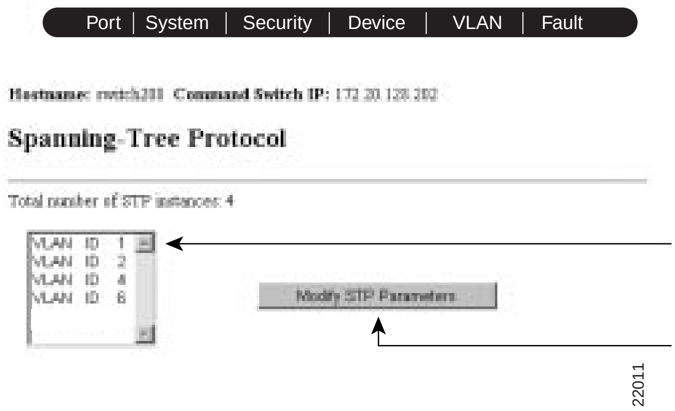
You can also create redundant links between switches by using EtherChannel port groups. See the “Creating EtherChannel Port Groups” section on page 3-21 for more information on creating port groups.

Accelerating Aging to Retain Connectivity

The default for aging dynamic addresses is 5 minutes. However, a reconfiguration of the spanning tree can cause many station locations to change. Because these stations could be unreachable for 5 minutes or more, the address-aging time is accelerated so that station addresses can be dropped from the address table and then relearned. The accelerated aging is the same as the forward-delay parameter value when STP reconfigures.

Because each VLAN is a separate instance of STP, the switch accelerates aging on a per-VLAN basis. A reconfiguration of STP on one VLAN can cause the dynamic addresses learned on that VLAN to be subject to accelerated aging. Dynamic addresses on other VLANs can be unaffected and remain subject to the aging interval entered for the switch.

Figure 3-26 Spanning-Tree Protocol (Selection)



Hostname: switch211 **Command Switch IP:** 172.20.128.202

Spanning-Tree Protocol

Total number of STP instances: 4

Each VLAN is a separate instance of STP.

Select a VLAN and click here.

Disabling STP Protocol

STP is enabled by default. Disable STP only if you are sure there are no loops in the network topology. With STP disabled and loops present in the topology, network performance is degraded by excessive traffic and indefinite packet duplication.

Changing STP Parameters for a VLAN

To change STP parameters for a VLAN, select **Device>Spanning-Tree Protocol** from the menu bar, select the VLAN ID of the STP instance to change, and click **Modify STP Parameters**.

In Figure 3-27, the parameters under the heading Current Spanning-Tree Root are read-only and could be defined on another switch. The MAC Address field shows the MAC address of the switch currently acting as the root. The parameters under the heading Spanning-Tree Options are the values that this switch would use as the root switch.

The following fields (see Figure 3-27) define how your switch responds when STP reconfigures itself.

Protocol Implementation of STP to use.

Select one of the menu items: DEC, IBM, or IEEE. The default is IEEE.

Priority Value used to identify the root bridge. The bridge with the **lowest value** has the highest priority and is selected as the root.

Enter a number from 0 to 65535.

Max age Number of seconds a bridge waits without receiving STP configuration messages before attempting a reconfiguration. This parameter takes effect when a bridge is operating as the root bridge. Bridges not acting as the root use the root-bridge Max age parameter.

Enter a number from 6 to 200.

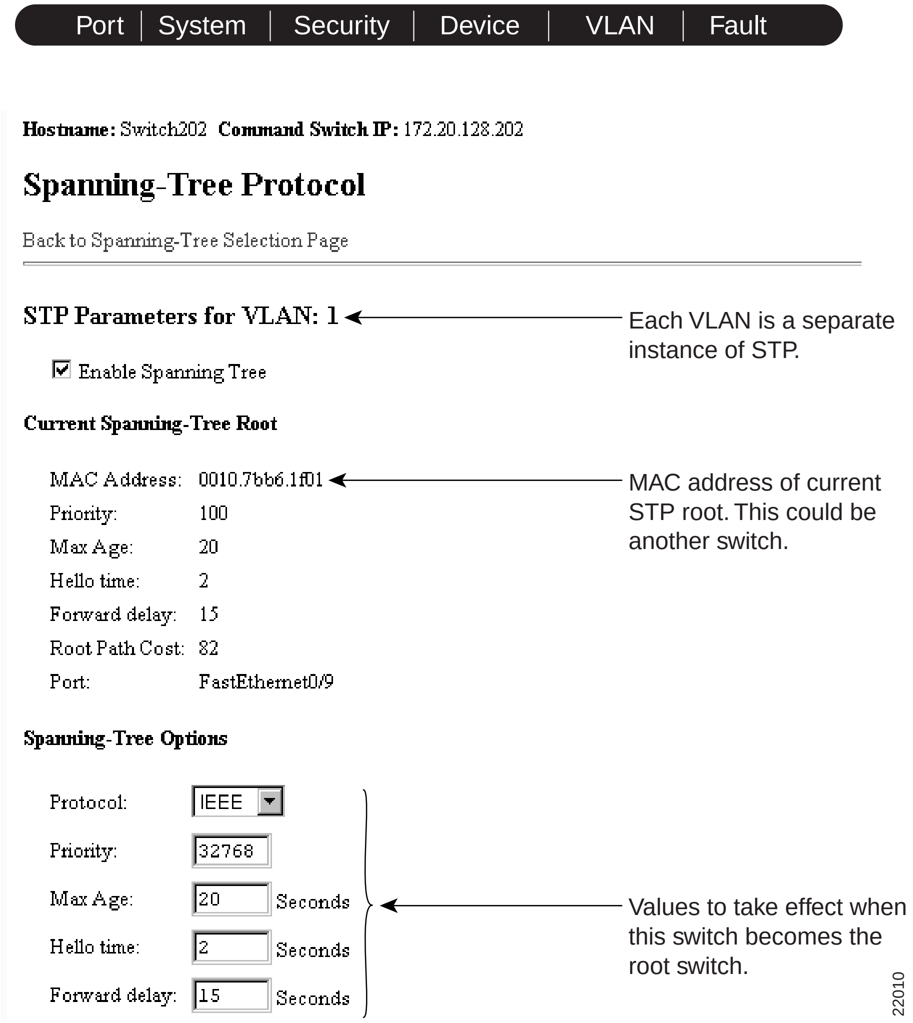
Hello Number of seconds between the transmission of STP configuration messages. Bridges not acting as a root bridge use the root-bridge Hello-time value.

Enter a number from 1 to 10.

Forward Delay Number of seconds a port waits before changing from its STP learning and listening states to the forwarding state. This wait is necessary so that other switches on the network ensure no loop is formed before they allow the port to forward packets.

Enter a number from 4 to 200.

Figure 3-27 Spanning-Tree Protocol (Part 1)



Hostname: Switch202 **Command Switch IP:** 172.20.128.202

Spanning-Tree Protocol

Back to Spanning-Tree Selection Page

STP Parameters for VLAN: 1

☑ Enable Spanning Tree

Current Spanning-Tree Root

MAC Address:	0010.7bb6.1f01
Priority:	100
Max Age:	20
Hello time:	2
Forward delay:	15
Root Path Cost:	82
Port:	FastEthernet0/9

Spanning-Tree Options

Protocol:	IEEE	
Priority:	32768	
Max Age:	20	Seconds
Hello time:	2	Seconds
Forward delay:	15	Seconds

Each VLAN is a separate instance of STP.

MAC address of current STP root. This could be another switch.

Values to take effect when this switch becomes the root switch.

Changing STP Port Parameters

The ports listed on this page belong to the VLAN selected at the top of the page.

To change STP options port options, select **Device>Spanning-Tree Protocol** from the menu bar, select the VLAN ID, and click **Modify STP Parameters**.

Path Cost — A lower path cost represents higher-speed transmission. This can affect which port remains enabled in the event of a loop.

Enter a number from 1 to 65535. The default is 100 for 10 Mbps, 19 for 100 Mbps, 14 for 155 Mbps (ATM), 4 for 1 Gbps, 2 for 2 Gbps, and 1 for interfaces with speeds greater than 10 Gbps.

Priority — Number used to set the priority for a port. A higher number has higher priority.

If you are using a DEC-type-STP, enter a number from 0 to 255.

If you are using an IEEE-type-STP, enter a number from 0 to 65535.

Use the following fields (see Figure 3-28) to check the status of ports that are not forwarding due to STP:

Port — The interface and port number. FastEthernet0/1 refers to port 1x.

State — The current state of the port. A port can be in one of the following states:

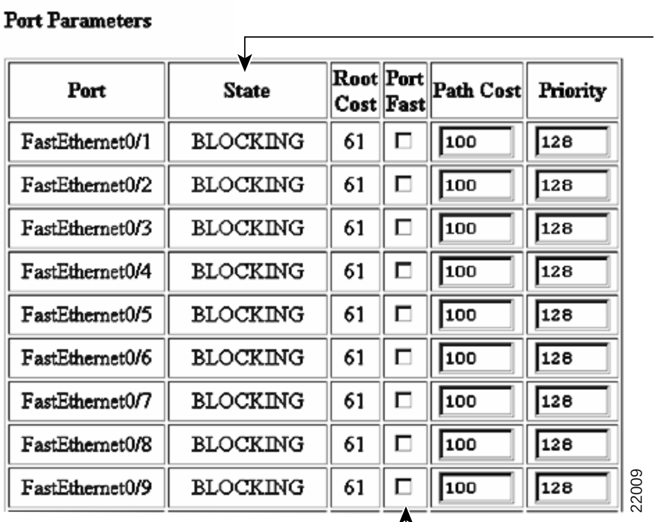
- Blocking — Port is not participating in the frame-forwarding process and is not learning new addresses.
- Listening — Port is not participating in the frame-forwarding process, but is progressing towards a forwarding state. The port is not learning addresses.
- Learning — Port is not forwarding frames but is learning addresses.
- Forwarding — Port is forwarding frames and learning addresses.
- Disabled — Port has been removed from STP operation.

Enabling the Port Fast Option

The Port Fast option brings a port directly from a blocking state into a forwarding state. The only time a port with the Port Fast option enabled goes through the normal cycle of STP status changes is when the switch is restarted. Use this option when a port is connected to a workstation or server and cannot contribute to bridging loops.

Caution Enabling this option on a port connected to a switch or hub could prevent STP from detecting and disabling loops in your network.

Figure 3-28 Spanning-Tree Protocol (Part 2)



Port Parameters

Port	State	Root Cost	Port Fast	Path Cost	Priority
FastEthernet0/1	BLOCKING	61	□	100	128
FastEthernet0/2	BLOCKING	61	□	100	128
FastEthernet0/3	BLOCKING	61	□	100	128
FastEthernet0/4	BLOCKING	61	□	100	128
FastEthernet0/5	BLOCKING	61	□	100	128
FastEthernet0/6	BLOCKING	61	□	100	128
FastEthernet0/7	BLOCKING	61	□	100	128
FastEthernet0/8	BLOCKING	61	□	100	128
FastEthernet0/9	BLOCKING	61	□	100	128

Shows current STP state of port.

Select to accelerate STP reconfiguration if port is connected to an end station.

CLI Commands for Enabling STP Port Fast

Enabling this option on a port connected to a switch or hub could prevent STP from detecting and disabling loops in your network. Beginning in privileged EXEC mode, follow these steps to enable the Port Fast option:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port to be configured.	**interface** *interface*
Step 3	Enable the Port Fast feature for the port.	**spanning-tree portfast**
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entry.	**show running-config**

For more information on IOS Release 11.2(8)SA6, see the *Cisco IOS Desktop Switching Command Reference.* The complete IOS Release 11.2(8) documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 11.2**.

Creating and Maintaining VLANs

Use the VLAN Membership page (Figure 3-29) to assign ports to VLANs.

To display this page, select **VLAN>VLAN Membership** from the menu bar.

Understanding VLANs

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to those stations within the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or bridge.

Because a VLAN is considered a separate logical network, it contains its own bridge MIB information and can support its own implementation of the Spanning-Tree Protocol (STP). The following switches can support up to 250 VLANs, but there only 64 possible instances of STP:

WS-C3524-XL-EN
WS-C3524-XL-A
WS-C3512-XL-EN
WS-C3512-XL-A
WS-C3508G-XL-A
WS-C3508G-XL-EN
WS-C2912MF-XL
WS-C2924M-XL-A
WS-C2924M-XL-EN

All other switches supported by this IOS release can support 64 VLANs. VLANs are identified with a number between 1 and 1001.

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

When a port belongs to a VLAN, the switch learns and manages the addresses associated with the port on a per-VLAN basis. See the “Managing the MAC Address Tables” section on page 3-49 for more information.

Assigning Ports to VLANs

By default, all ports are static-access ports assigned to VLAN 1, which is also referred to as the Management VLAN. VLAN 1 is also the interface to the switch itself. If you are using SNMP or CVSM to manage the switch, ensure that the port through which you are connected to the switch is in VLAN 1.

A port can be in one of these modes:

- Static-access: the port belongs to one VLAN.
- Multi-VLAN: the port can belong to more than one VLAN.

When you assign a port to a VLAN, you define the port as a multi-VLAN or a static-access port and enter a VLAN ID for it. If you change the VLAN ID on a port that belongs to a port group, the VLAN ID for all the ports in that group is also changed.

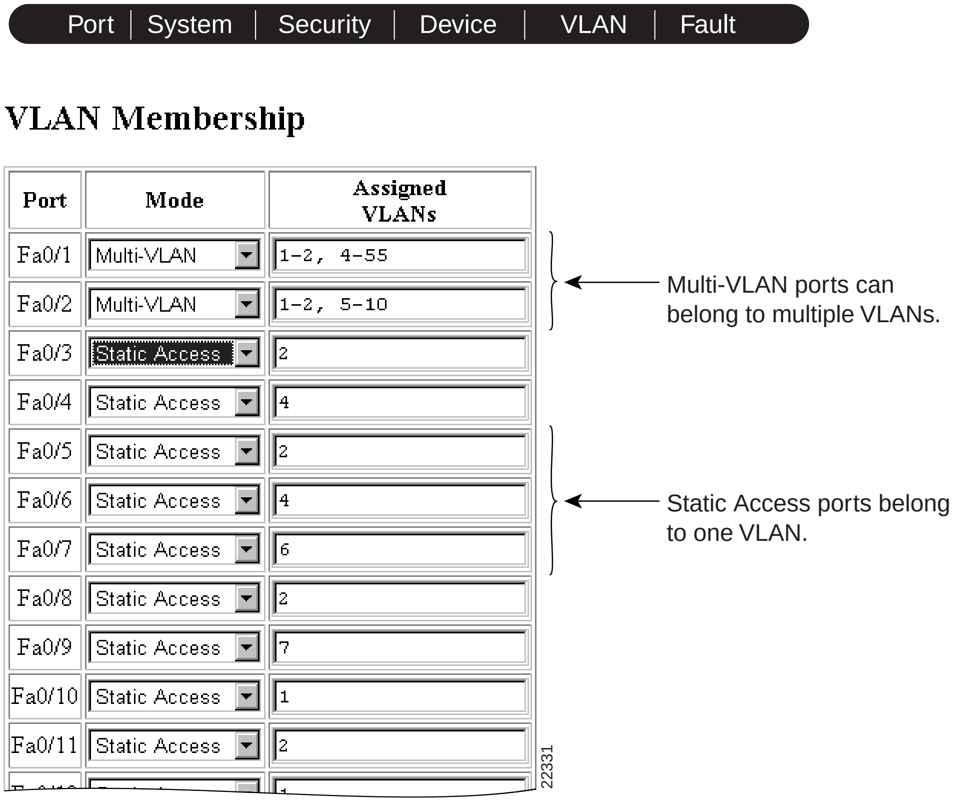
CLI Commands for Assigning Static Access Ports to a VLAN

Beginning in privileged EXEC mode, follow these steps to assign a port for static-access VLAN membership:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port to be added to the VLAN.	**interface** *interface*
Step 3	Enter the VLAN membership mode for static-access ports.	**switchport mode access**
Step 4	Assign the port to a VLAN.	**switchport access vlan 2**
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries.	**show interface** *interface-id* **switchport**

For more information on IOS Release 11.2(8)SA6, see the *Cisco IOS Desktop Switching Command Reference.* The complete IOS Release 11.2(8) documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 11.2**.

Figure 3-29 VLAN Membership



VLAN Membership

Port	Mode	Assigned VLANs
Fa0/1	Multi-VLAN	1-2, 4-55
Fa0/2	Multi-VLAN	1-2, 5-10
Fa0/3	Static Access	2
Fa0/4	Static Access	4
Fa0/5	Static Access	2
Fa0/6	Static Access	4
Fa0/7	Static Access	6
Fa0/8	Static Access	2
Fa0/9	Static Access	7
Fa0/10	Static Access	1
Fa0/11	Static Access	2

Multi-VLAN ports can belong to multiple VLANs.

Static Access ports belong to one VLAN.

VLAN Membership for an ATM Port

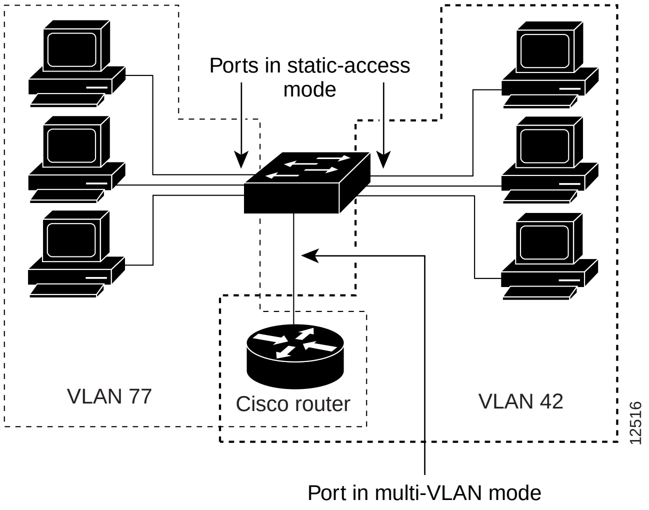
Using the ATM module CLI, you can map the LAN emulation (LANE) client to a VLAN or bind one or more permanent virtual connections (PVCs) to a VLAN. The VLAN ID is then displayed in the Assigned VLANs column of the VLAN Membership page. Using standard edition software, an ATM port can only be a static-access port. Using Enterprise Edition Software, an ATM port can only be a trunk port. An ATM port can never be a multi-VLAN port.

Overlapping VLANs

A multi-VLAN port connected to a router can link two or more VLANs. Intra-VLAN traffic stays within the boundaries of the respective VLANs, and connectivity between VLANs is via the router connected to the multi-VLAN port, as shown in Figure 3-30.

A multi-VLAN port functions normally in all its assigned VLANs. For example, when a multi-VLAN port receives an unknown MAC address, all the VLANs to which the port belongs learn the address. Multi-VLAN ports also respond to the STP messages generated by the different instances of STP in each VLAN.

Figure 3-30 Two VLANs Sharing a Port Connected to a Router



Caution Avoid unpredictable STP behavior by strictly limiting the connection of multi-VLAN ports to routers or servers.

CLI Commands for Assigning Multi-VLAN Ports to VLANs

To avoid loss of connectivity, do not connect multi-VLAN ports to hubs or switches. Connect multi-VLAN ports to routers or servers.

Beginning in privileged EXEC mode, follow these steps to assign ports for multi-VLAN membership:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port to be added to the VLAN.	**interface** *interface*
Step 3	Enter the VLAN membership mode for multi-VLAN ports.	**switchport mode multi**
Step 4	Assign the port to more than one VLAN. Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.	**switchport multi vlan add** *vlan-list*
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries.	**show interface** *interface-id* **switchport**

For more information on IOS Release 11.2(8)SA6, see the *Cisco IOS Desktop Switching Command Reference.* The complete IOS Release 11.2(8) documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 11.2**.

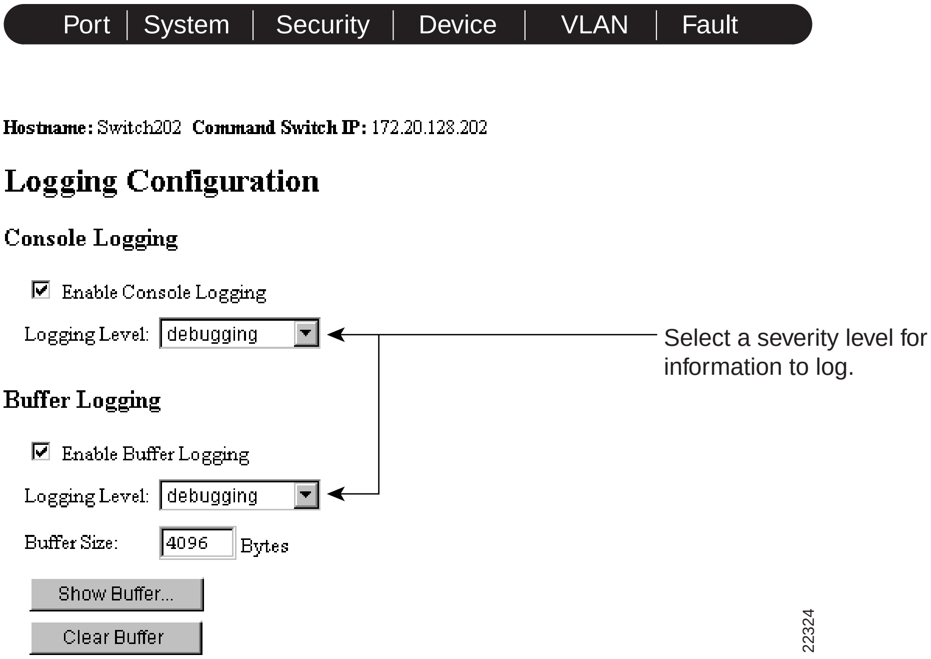
Configuring the Switch to Log Information

Use the Logging Configuration page (Figure 3-31 and Figure 3-32) to define the logging type and the severity level of information that the switch logs. The switch can generate log messages when the configuration changes and when certain network or switch events occur.

To display this page, select **Fault>Logging Config** from the menu bar.

This guide describes the use of IOS commands that have been created or changed for use with switches that support IOS Release 11.2(8)SA6. For information on other IOS Release 11.2(8) commands, see the IOS documentation set available from the CCO home page by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 11.2Cisco IOS Release 11.2**.

Figure 3-31 Logging Configuration (Part 1)



Hostname: Switch202 **Command Switch IP:** 172.20.128.202

Logging Configuration

Console Logging

☑ Enable Console Logging

Logging Level: debugging

Buffer Logging

☑ Enable Buffer Logging

Logging Level: debugging

Buffer Size: 4096 Bytes

Select a severity level for information to log.

Selecting a Logging Option

You can select one of the following options for recording log information:

Console Logging
Write log information to the management console.

Buffer Logging
Write log information to a buffer in Flash memory. Enter the size of the buffer in the Buffer Size field. The recommended buffer size is 32 KB.

The buffer maintains information on a first-in, first-out basis. If the buffer is full and you click **Show Buffer**, the most recent data is always displayed.

File Logging
Maintain a log file on an external server or in Flash memory. If the switch fails, it writes information about the cause of the failure to this file before functionality is lost. Click **Help** for instructions on how to configure this parameter.

Syslog
Use the UNIX syslog facility to manipulate log information written to a UNIX host. Log information sent to the UNIX host is then managed according to the facility. Click **Help** for instructions on how to configure this parameter.

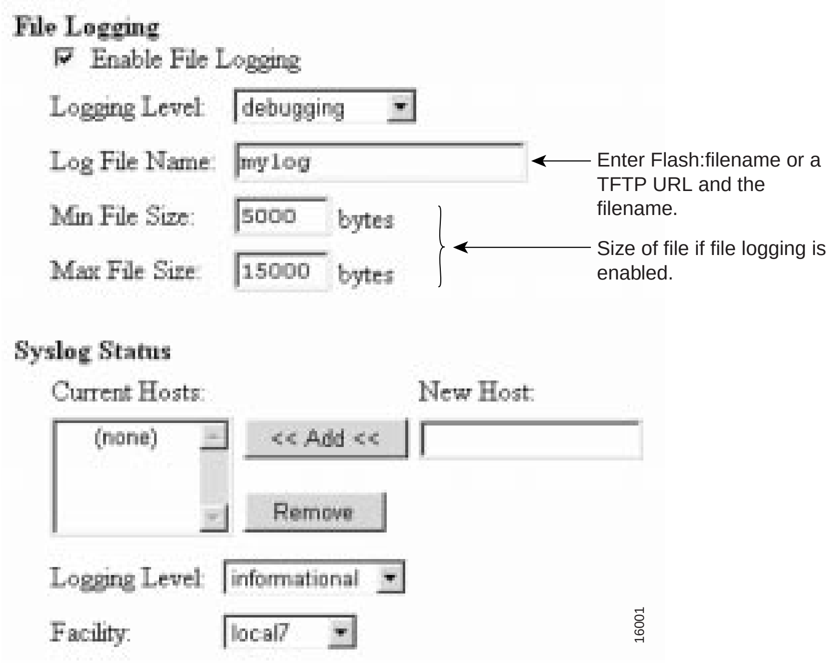
Defining a Severity Level

The switch can log eight levels of messages. When you select a logging level, the switch logs all syslog messages of that level and above. The default level is “Errors.” In all cases, the severity level defines the amount of detail to be logged.

Select a level from one of the following choices on the Logging Level drop-down list:

Emergencies	The switch is at risk of failing.
Alert	A condition exists that should be corrected immediately.
Critical	A critical condition exists, such as a device error.
Errors	Errors.
Warnings	Warning messages.
Notifications	Conditions that are not errors, but that could require special handling.
Information	Informational messages.
Debugging	Messages only used for debugging.

Figure 3-32 Logging Configuration (Part 2)



File Logging

☑ Enable File Logging

Logging Level: debugging

Log File Name: mylog

Min File Size: 5000 bytes

Max File Size: 15000 bytes

Syslog Status

Current Hosts: (none)

New Host:

Logging Level: informational

Facility: local7

Enter Flash:filename or a TFTP URL and the filename.

Size of file if file logging is enabled.