CHAPTER 3

Managing Your Switches

You can use the IOS Release 12.0(5)XP software to manage a single switch, a stack 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 this software release and how you can change them.

This chapter describes how to manage a single switch by using the following methods:

- Cisco Switch Network View, a graphical application that displays a map of the devices that are connected to your switch.
- Cisco Visual Switch Manager (CVSM), a graphical application for monitoring the switch, configuring ports and other features, and upgrading the switch software.

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

- Cisco IOS command-line interface (CLI)

  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 the 2900 and 3500 XL switches. These commands are further described in the *Cisco IOS Desktop Switching Command Reference* (online only). For information on other IOS Release 12.0 commands, refer to 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 12.0**.

For information on clustering, see Chapter 4, “Managing Clusters of Switches.”

Changing Default Settings

You can configure the software features of this 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	Web Interface or Menu Option, and Section in this Guide	Equivalent IOS CLI Procedure
Network Management			
Creating clusters	None	Cluster Builder “Creating Clusters” section on page 4-5	“CLI Procedure for Creating the Cluster” section on page 4-11
Removing cluster members	None	Cluster Builder “Adding and Removing Member Switches” section on page 4-12	“CLI Procedure for Removing Member Switches” section on page 4-15
Upgrading cluster software	Enabled	Cluster Manager “Upgrading Software for a Group of Switches” section on page 4-27	“CLI Procedure for Upgrading Catalyst 2900 or 3500 XL Member Switches” section on page 4-29
Displaying reports	Enabled	Cluster Manager and Cluster Builder “Displaying Device Reports and Graphs” section on page 4-42	—
Displaying VLAN membership information	None	Cluster Manager “Displaying VLAN Membership” section on page 4-26	—
Configuring SNMP community strings and trap managers	None	Cluster Manager “Configuring SNMP” section on page 4-31	—
Configuring a port	None	Cluster Manager “Configuring Ports” section on page 4-21	—

Table 3-1 Default Settings and Where to Find Them (continued)

Feature	Default Setting	Web Interface or Menu Option, and Section in this Guide	Equivalent IOS CLI Procedure
Device Management			
Switch IP address, subnet mask, and default gateway	0.0.0.0	CVSM: System>IP Management "Configuring IP Information" section on page 3-50	"CLI Procedure for Assigning IP Information to the Switch" section on page 3-53
Management VLAN	VLAN 1	CVSM: System>IP Management "Configuring the Management VLAN Interface" section on page 3-54	"CLI Procedure for Configuring the Management VLAN Interface through a Console Connection" section on page 3-56
Domain name	None	CVSM: System>IP Management "Specifying a Domain Name and Configuring the DNS" section on page 3-58	Documentation set for Cisco IOS Release 12.0 on CCO
Cisco Discovery Protocol (CDP)	Enabled	CVSM: Device>Cisco Discovery Protocol "Configuring the Cisco Discovery Protocol" section on page 3-80	Documentation set for Cisco IOS Release 12.0 on CCO
Address Resolution Protocol (ARP)	Enabled	CVSM: System>ARP Table "Managing the ARP Table" section on page 3-65	Documentation set for Cisco IOS Release 12.0 on CCO
System Time Management	None	CVSM: System>System Time Management "Setting the System Date and Time" section on page 3-46	Documentation set for Cisco IOS Release 12.0 on CCO
Static address assignment	None assigned	CVSM: Security>Address Management "Adding and Removing Static Addresses" section on page 3-73	"CLI Procedure for Adding Static Addresses" section on page 3-75

Table 3-1 Default Settings and Where to Find Them (continued)

Feature	Default Setting	Web Interface or Menu Option, and Section in this Guide	Equivalent IOS CLI Procedure
Dynamic address management	Enabled	CVSM: Security>Address Management "Managing the MAC Address Tables" section on page 3-67 and "Changing the Address Aging Time" section on page 3-70	"CLI Procedure for Configuring the Aging Time" section on page 3-70 "CLI Procedure for Removing Dynamic Address Entries" section on page 3-71
Device Management (cont)			
Cisco Switch Network View	Enabled	"Managing Switches through Switch Network View" section on page 3-9	—
VLAN membership	Static-access ports in VLAN 1	CVSM: VLAN>VLAN Membership "Assigning Ports to VLANs" section on page 3-103	"CLI Procedure for Assigning Static-Access Ports to a VLAN" section on page 3-104 "CLI Procedure for Assigning Ports for Multi-VLAN Membership" section on page 3-105
Performance			
Autonegotiation of duplex mode and port speeds	Enabled	CVSM: Port>Port Configuration "Configuring Port Parameters" section on page 3-23	"CLI Procedure for Setting Speed and Duplex Parameters" section on page 3-24 "CLI Procedure for Setting Speed and Duplex Parameters" section on page 3-24
Gigabit Ethernet flow control	Any	CVSM: Port>Port Configuration "Configuring Ports" section on page 3-20	"CLI Procedure for Configuring Flow Control on Gigabit Ethernet Ports" section on page 3-25
Flooding Control			

Table 3-1 Default Settings and Where to Find Them (continued)

Feature	Default Setting	Web Interface or Menu Option, and Section in this Guide	Equivalent IOS CLI Procedure
Broadcast storm control	Disabled	CVSM: Port>Flooding Controls “Enabling Broadcast Storm Control” section on page 3-35	“CLI Procedure for Enabling Broadcast Storm Control” section on page 3-36
Flooding unknown unicast and multicast packets	Enabled	CVSM: Port>Flooding Controls “Blocking Flooded Traffic on a Port” section on page 3-37	“CLI Procedure for Blocking Flooded Traffic on a Port” section on page 3-38
Flooding Control (cont)			
Network port	Disabled	CVSM: Port>Flooding Controls “Enabling a Network Port” section on page 3-34	“CLI Procedure for Enabling a Network Port” section on page 3-34
Cisco Group Management Protocol (CGMP)	Enabled	CVSM: Device>Cisco Group Management Protocol “Controlling IP Management Packets through CGMP” section on page 3-83	“CLI Procedure for Enabling the CGMP Fast Leave Feature” section on page 3-85 “CLI Procedure for Changing the Router Hold-Time” section on page 3-86 “CLI Procedure for Removing Multicast Groups” section on page 3-87
Network Redundancy			

Table 3-1 Default Settings and Where to Find Them (continued)

Feature	Default Setting	Web Interface or Menu Option, and Section in this Guide	Equivalent IOS CLI Procedure
Spanning-Tree Protocol	Enabled	CVSM: Device>Spanning-Tree Protocol “Configuring the Spanning-Tree Protocol” section on page 3-88	“CLI Procedure for Disabling STP Protocol” section on page 3-90 “CLI Procedure for Changing the Path Cost” section on page 3-99 “CLI Procedure for Changing the Port Priority” section on page 3-100 “CLI Procedure for Enabling STP Port Fast” section on page 3-99
Port grouping	None assigned	CVSM: Port>Port Grouping (EC) “Creating EtherChannel Port Groups” section on page 3-26	“CLI Procedure for Creating EtherChannel Port Groups” section on page 3-28
Diagnostics			
SPAN port monitoring	Disabled	CVSM: Port>Switch Port Analyzer (SPAN) “Enabling Switch Port Analyzer” section on page 3-29	“CLI Procedure for Enabling Switch Port Analyzer” section on page 3-31
Console, buffer, and file logging	Disabled	CVSM: Fault>Logging Config “Configuring the Switch to Log Information” section on page 3-107	Documentation set for Cisco IOS Release 12.0 on CCO
Remote monitoring (RMON)	Disabled	— “Configuring the Switch for Remote Monitoring” section on page 3-110	Documentation set for Cisco IOS Release 12.0 on CCO
Security			
Password	None	CVSM: Visual Switch Manager Home “Changing the Password” section on page 3-15	“Recovering from a Lost or Forgotten Password” section on page 5-4

Table 3-1 Default Settings and Where to Find Them (continued)

Feature	Default Setting	Web Interface or Menu Option, and Section in this Guide	Equivalent IOS CLI Procedure
Addressing security	Disabled	CVSM: Security>Address Management “Adding Secure Addresses” section on page 3-71	“CLI Procedure for Adding Secure Addresses” section on page 3-72
Trap manager	0.0.0.0	CVSM: System>SNMP Configuration “Adding Trap Managers” section on page 3-62	“CLI Procedure for Adding a Trap Manager” section on page 3-64
Community strings	public	CVSM: System>SNMP Configuration “Entering Community Strings” section on page 3-62	Documentation set for Cisco IOS Release 12.0 on CCO
Port security	Disabled	CVSM: Security>Port Security “Enabling Port Security” section on page 3-77	“CLI Procedure for Enabling Port Security” section on page 3-79

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	Connect to Cluster?
ATM Port	—	No	No	No	No	No	Yes
Port Group	No	—	No	No	Yes	Yes[2]	Yes
Port Security	No	No	—	No	No	No	Yes
SPAN Port	No[3]	No	No	—	No	No	Yes
Multi-VLAN Port	No	Yes	No	No	—	Yes	Yes
Network Port	No	Yes (source-based only)	No	No	Yes	—	No[4]
Connect to Cluster	Yes	Yes	Yes	Yes	Yes	No	—

[1] Catalyst 2900 XL switches only.

[2] Cannot be in a destination-based port group.

[3] An ATM port cannot be a monitor port but can be monitored.

[4] Cannot connect cluster members to the command switch.

Saving Changes to the Startup Configuration

The configuration file that loads when the switch is restarted is stored in Flash memory. The 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. The CVSM procedure is described in the "Reloading and Upgrading the Switch Software" section on page 3-40. The CLI procedure is described in the "Working with Files in Flash Memory" section on page 2-37.

Managing Switches through Switch Network View

Switch Network View extends web-based network management to the other devices in your network. By exchanging Cisco Discovery Protocol (CDP) messages with attached CDP-enabled devices, Switch Network View graphically displays the surrounding star topology that consists of 2900 and 3500 XL switches and Cisco edge devices.

Supported switches must be running the IOS Release 12.0(5)XP or 11.2(8.x)SA6. Catalyst 2900 XL switches with 4 MB of DRAM must be running IOS Release 11.2(8.x)SA6. For more information, see Table 1-1 on page 1-4. In addition, you need to enable SNMP and set the community string to **public** on all stack members.

Switch Network View differs from Cluster Management in the following ways:

- You must assign an IP address to each stack member.
- You must connect your switches in a star topology with the primary switch at the center. Switch Network View does not support daisy-chained switch topologies.
- Up to four directly connected supported switches can be stack members.

Understanding a Switch Network View Stack

The center node in a star topology acts as a *primary* switch in Switch 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 about the stack from the Switch Network View page and the Visual Stack page.

If more than four switches are connected, Switch Network View displays only the four connected to the lowest port numbers of the primary switch. All other devices are considered edge devices.

For a complete description of the Switch Network View interface, see “Using Switch Network View” section on page 2-13.

Displaying the Switch Network View Page

The Switch 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 Switch 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 Switch Network View page:

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

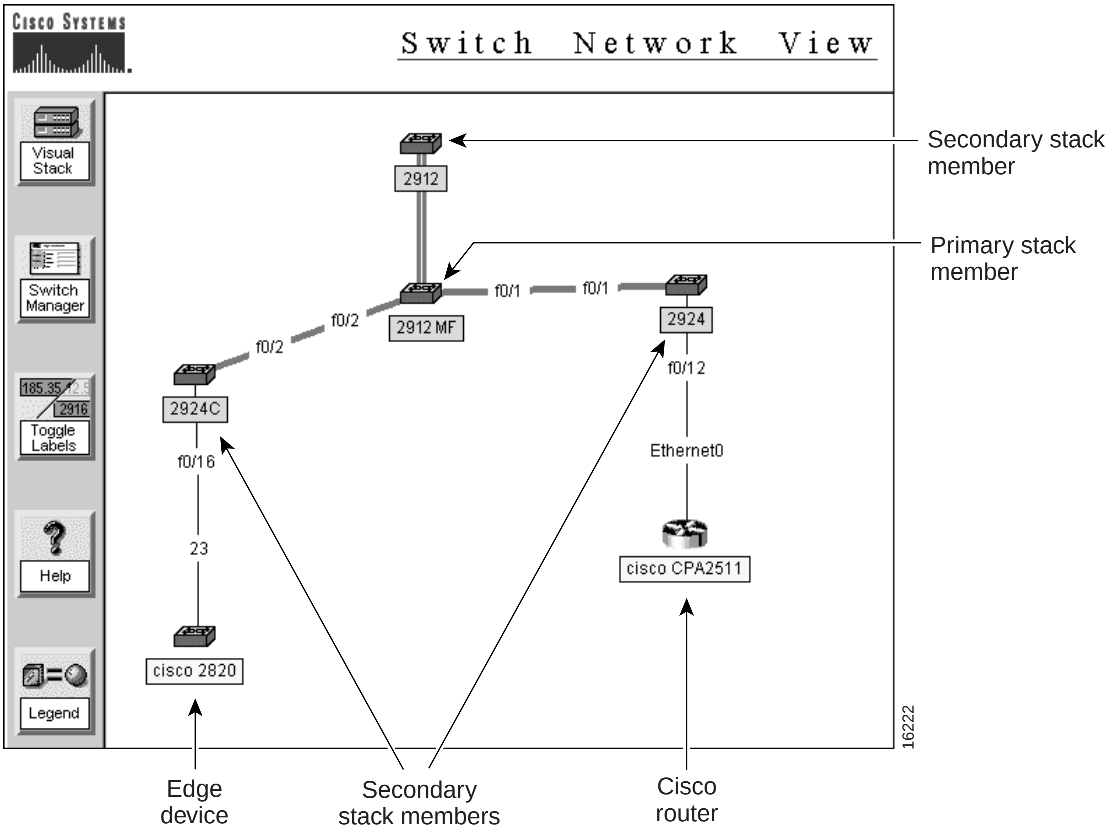
You will see the Switch Network View button only if the switch is not part of a cluster.

Step 2 When prompted, enter the password for each switch in the stack.

You do not need to enter a username.

You can launch Switch Network View from any member switch but the topology that is shown may not display all the switch members. Recall that Switch Network View displays directly connected members one hop from the primary switch. Therefore, pointing your browser at the primary switch in a star topology ensures the most complete view of the network.

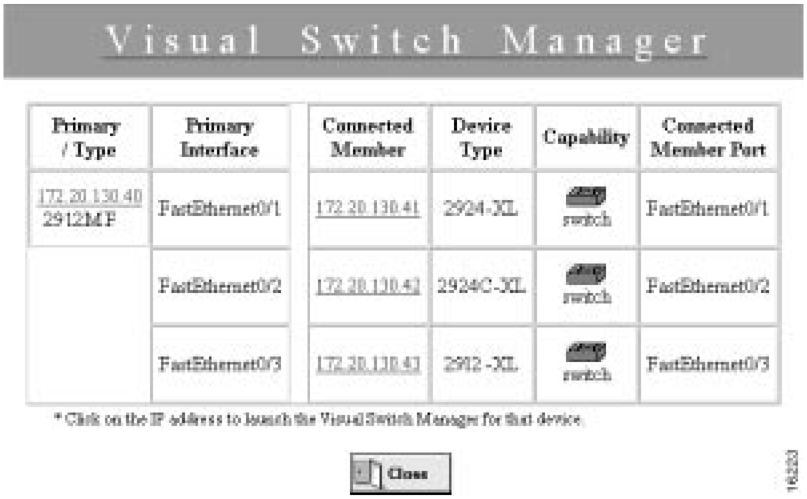
Figure 3-1 Switch Network View Page



Displaying Switch Connection Information

Figure 3-2 shows connection information for the switches being managed by Switch Network View. Click on the **Switch Manager** button on the Switch Network View page to display this table.

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 Visual Stack

The visual stack is an image of up to five 2900 or 3500 XL switches or both (Figure 3-3) with the primary switch at the top. This stack contains the same switches as those on the Switch Network View page (Figure 3-1), 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 application.

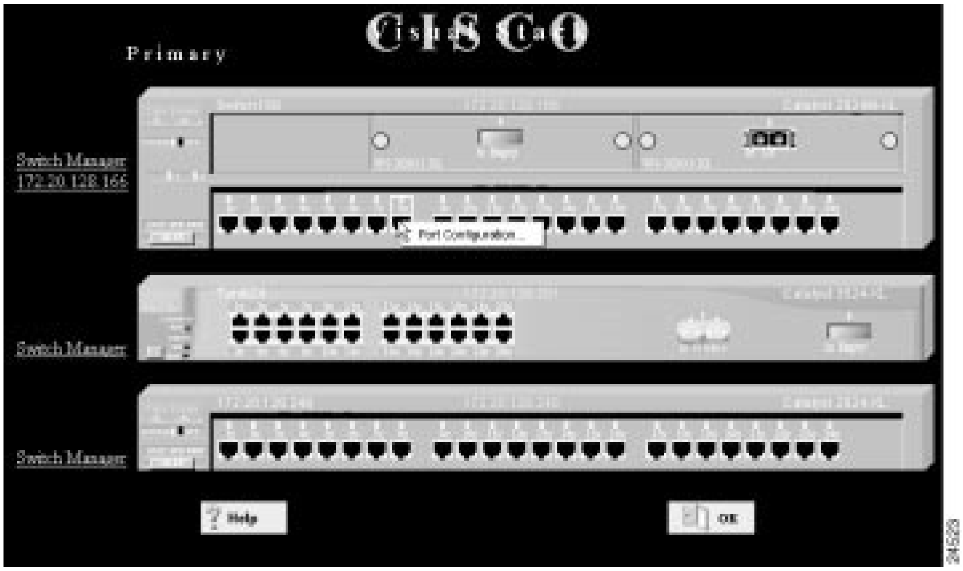
Follow these steps to display the visual stack:

Step 1 Display the Switch Network View page as described in the “Displaying the Switch Network View Page” section on page 3-10.

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 or higher.

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, double-click a port to launch the Port Configuration window, which shows the port settings and status. (You can also right-click a port to display the pop-up menu. Select **Port Configuration** to display the Port Configuration pop-up window.) 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 3-18.

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

Managing Your Switch through 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

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

Use this page to perform the following tasks:

- Change the enable secret password
- Enable the switch as a command switch
- Display Cluster Management or Switch Network View
- Monitor switch LEDs
- Configure ports

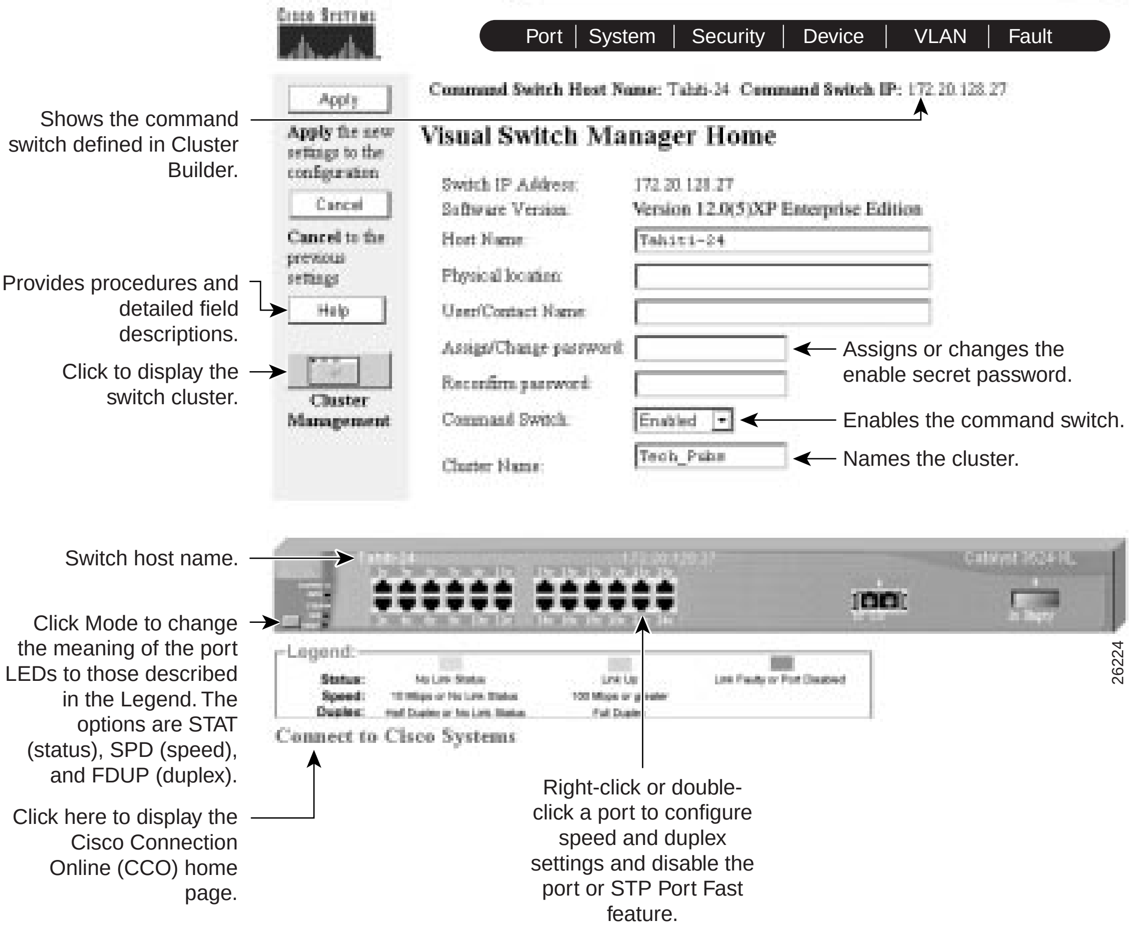
Changing the Password

If you change the enable secret password on this page, your connection with the switch breaks, and the browser prompts you for the new password. For information on how to change the password, click **Help**. If you have forgotten your password, see the "Recovering from a Lost or Forgotten Password" section on page 5-4.

CLI Procedure for Changing the Password

This guide describes how to use the IOS commands that have been created or changed for switches that support IOS Release 12.0(5)XP. For information on other IOS commands, refer to 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 12.0**.

Figure 3-4 CVSM Home Page



Apply the new settings to the configuration

Cancel to the previous settings

Command Switch Host Name: Tahiti-24 **Command Switch IP:** 172.20.128.27

Visual Switch Manager Home

Switch IP Address: 172.20.128.27

Software Version: Version 12.0(5)XP Enterprise Edition

Host Name: Tahiti-24

Physical location:

User/Contact Name:

Assign/Change password:

Reconfirm password:

Command Switch: Enabled

Cluster Name: Tech_Pubs

Tahiti-24 172.20.128.27 Catalyst 3524 XL

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.

Assigns or changes the enable secret password.

Enables the command switch.

Names the cluster.

Switch host name.

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

Enabling the Switch as a Command Switch

If the switch is command-capable, you can enable it and name the cluster that it controls. After you enable the command switch, the Cluster Management button displays on the home page. Table 1-1 on page 1-4 lists the switches that can be command switches and those that can be command-enabled by a software upgrade.

CLI Procedure for Enabling the Command Switch and Naming the Cluster

Beginning in privileged EXEC mode, follow these steps to enable the command switch and name the cluster:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable and name the cluster. The name can be up to 31 characters.	**cluster enable** *name*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show cluster**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

Monitoring Port Settings

CVSM refreshes the switch image every 30 seconds to provide the most up-to-date information. 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.

You can also use the switch images in Cluster Manager to display VLAN membership information and detailed information about the links between switches. For more information, see Chapter 4, “Managing Clusters of Switches.”

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 lights when a module is installed in a modular switch.

Configuring Ports on the Switch Home Page

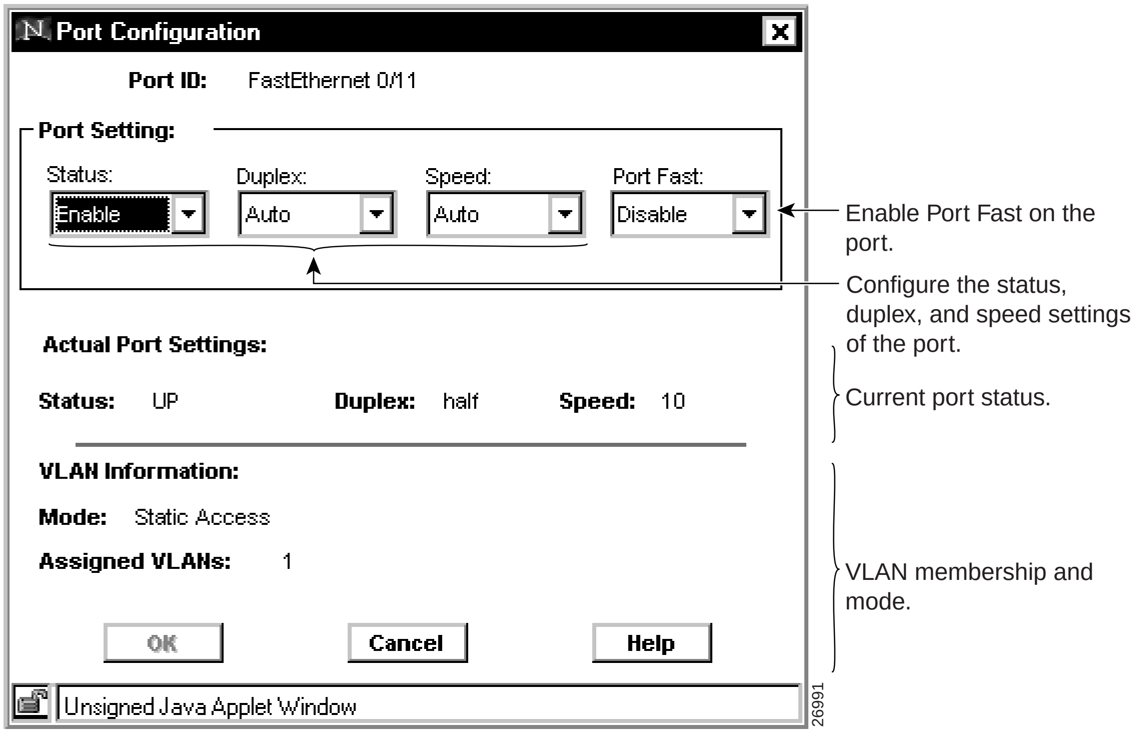
You configure a port by using one of the following methods:

- Right-click a port and select **Port Configuration** from the pop-up menu.
- Double-click a port to display the Port Configuration pop-up window.
- Select multiple ports by holding the **Ctrl** key and clicking more than one port. Then select **Port Configuration** from the pop-up menu.

Figure 3-5 shows the Port Configuration pop-up window, which has the same features as the Port Configuration window in Figure 3-6. The LEDs on the image of the switch reflect any changes you make. If your switch is part of a cluster, you can also configure the ports with the Cluster Management application. For more information, see Chapter 4, “Managing Clusters of Switches.”

This software release supports 10/100, Gigabit Ethernet, ATM, and Catalyst GigaStack Gigabit Interface Converters (GBICs). For defaults and guidelines for configuring the different types of ports, see the “Configuring Port Parameters” section on page 3-23.

Figure 3-5 Port Configuration Pop-up



Port ID: FastEthernet 0/11

Port Setting:

Status: Enable

Duplex: Auto

Speed: Auto

Port Fast: Disable

Actual Port Settings:

Status: UP **Duplex:** half **Speed:** 10

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

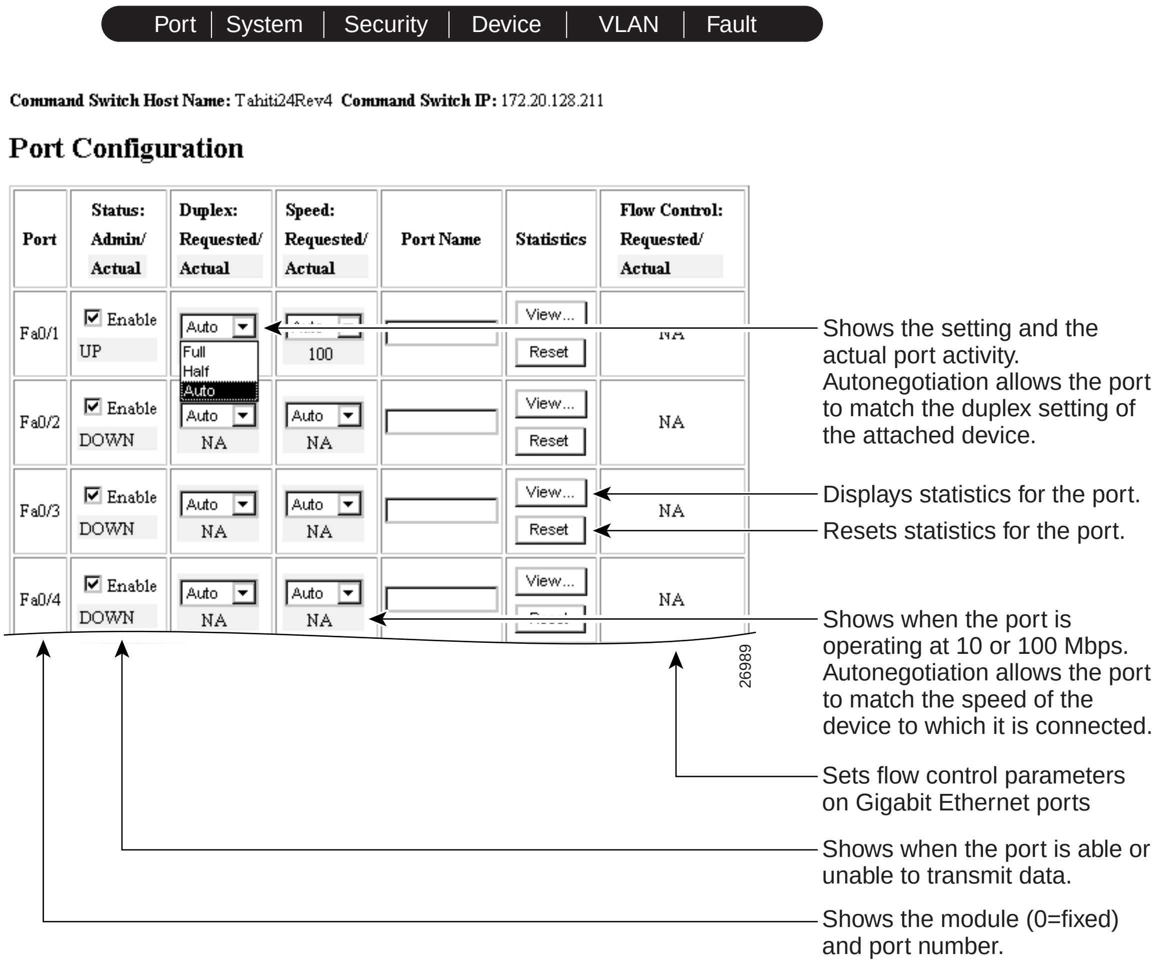
Use the Port Configuration page (Figure 3-6) to perform the following tasks:

- Enable and disable ports.
- Set the duplex, speed and Port Fast parameters.
- Configure flow control on Gigabit Ethernet ports.

Table 3-3 on page 3-22 describes the column headings and fields. The “Configuring Port Parameters” section on page 3-23 contains guidelines for using this page.

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

Figure 3-6 Port Configuration



Command Switch Host Name: Tahiti24Rev4 **Command Switch IP:** 172.20.128.211

Port Configuration

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

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.

Sets flow control parameters on Gigabit Ethernet ports

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

Field	Description
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 3-6, the port is a fixed port (0) and port number 1: Fa0/1. **Note** The port numbers for the double-row connectors on the 3500 XL switches increment from top to bottom and left to right.
Status: Admin/Actual	Administratively 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** (1000 Mbps) 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. Click **View** to display statistics.
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. 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 If you reconfigure the port through which you are managing the switch, an 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 port speed 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 these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

CLI Procedure for Configuring Flow Control on Gigabit Ethernet Ports

Beginning in privileged EXEC mode, follow these steps to configure flow control on a Gigabit Ethernet 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	Configure flow control for the port.	**flowcontrol** [**asymmetric** | **symmetric**]
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entries.	**show running-config**
Step 6	(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 these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

Creating EtherChannel Port Groups

Use the Port Group (EtherChannel) page (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 either 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.

For the restrictions that apply to port groups, see the “Managing Configuration Conflicts” section on page 3-7.

Understanding EtherChannel Port Grouping

This software release supports two different types of port groups: source-based forwarding port groups and destination-based forwarding port groups.

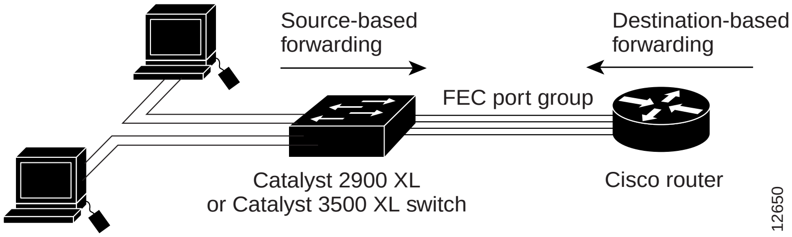
Source-based forwarding port groups distribute packets forwarded to the group based on the source address of incoming packets. You can configure up to eight ports in a source-based forwarding port group. Source-based forwarding is enabled by default.

Destination-based port groups distribute packets forwarded to the group based on the destination address of incoming packets. You can configure an unlimited number of ports in a destination-based port group.

You can create up to 12 port groups of all source-based, all destination-based, or a combination of source- and destination-based ports. All ports in the group must be of the same type; for example, they must be all source based or all destination based. You can independently configure port groups that link switches, but you must consistently configure both ends of a port group.

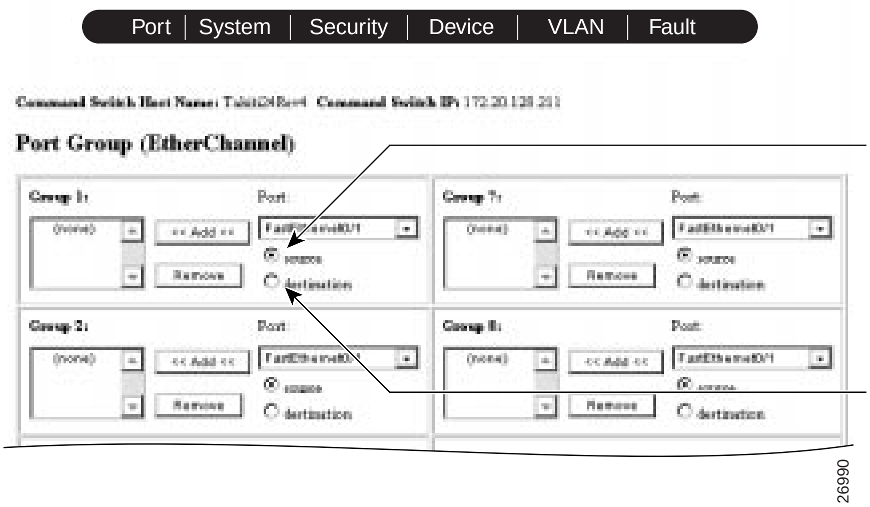
In Figure 3-7, a port group of two workstations communicates with a router. Because the router is a single-MAC address device, source-based forwarding ensures that the switch uses all available bandwidth to the router. The router is configured for destination-based forwarding because the large number of stations ensures that the traffic is evenly distributed through the port-group ports on the router.

Figure 3-7 Source-Based Forwarding


Source-based forwarding
Destination-based forwarding
FEC port group
Catalyst 2900 XL or Catalyst 3500 XL switch
Cisco router
12650

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)



Command Switch Host Name: Tahiti24Rev4 Command Switch IP: 172.20.128.211

Port Group (EtherChannel)

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 static address to forward 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 static address to forward 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 3-73.

CLI Procedure for Creating EtherChannel Port Groups

Beginning in privileged EXEC mode, follow these steps 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 these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

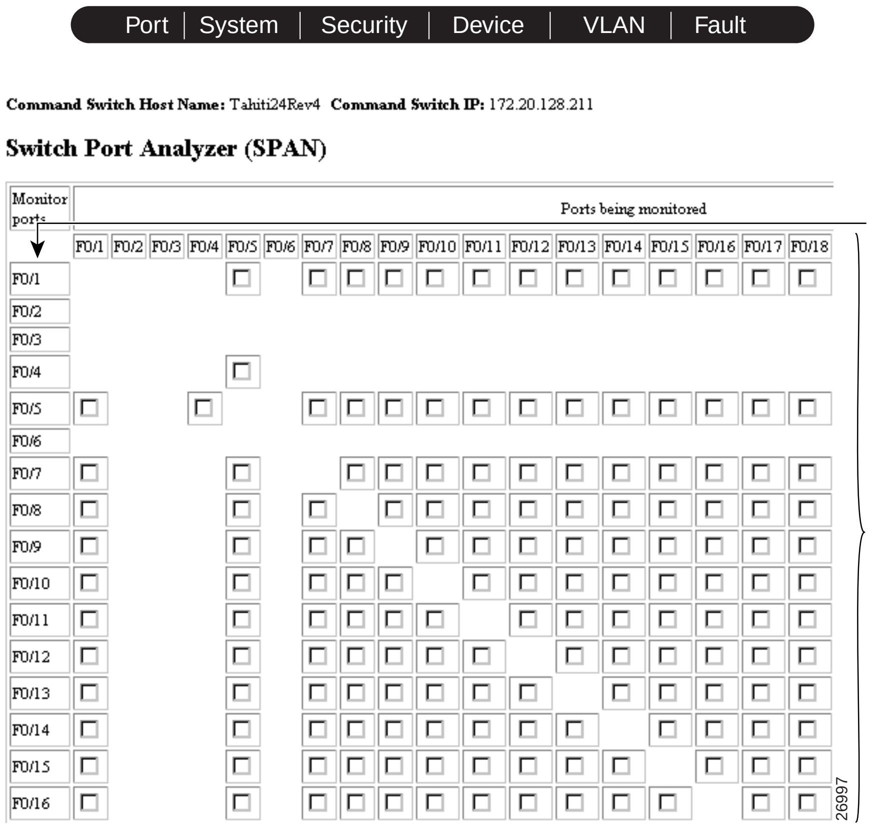
Enabling Switch Port Analyzer

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 3-7.

Figure 3-9 Switch Port Analyzer (SPAN)



Command Switch Host Name: Tahiti24Rev4 **Command Switch IP:** 172.20.128.211

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	F0/13	F0/14	F0/15	F0/16	F0/17	F0/18
F0/1					□		□	□	□	□	□	□	□	□	□	□	□	□
F0/2																		
F0/3																		
F0/4					□													
F0/5	□			□			□	□	□	□	□	□	□	□	□	□	□	□
F0/6																		
F0/7	□				□			□	□	□	□	□	□	□	□	□	□	□
F0/8	□				□		□		□	□	□	□	□	□	□	□	□	□
F0/9	□				□		□	□		□	□	□	□	□	□	□	□	□
F0/10	□				□		□	□	□		□	□	□	□	□	□	□	□
F0/11	□				□		□	□	□	□		□	□	□	□	□	□	□
F0/12	□				□		□	□	□	□	□		□	□	□	□	□	□
F0/13	□				□		□	□	□	□	□	□		□	□	□	□	□
F0/14	□				□		□	□	□	□	□	□	□		□	□	□	□
F0/15	□				□		□	□	□	□	□	□	□	□		□	□	□
F0/16	□				□		□	□	□	□	□	□	□	□	□		□	□

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

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

CLI Procedure for Enabling Switch Port Analyzer

Beginning in privileged EXEC mode, follow these steps to enable switch port analyzer:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port that acts as the monitor port.	**interface** *interface*
Step 3	Enable port monitoring on the port.	**port monitor** *interface*
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entries.	**show running-config**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

CLI Procedure for Disabling Switch Port Analyzer

Beginning in privileged EXEC mode, follow these steps to disable switch port analyzer:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the port number of the monitor port.	**interface** *interface*
Step 3	Disable port monitoring on the port.	**no port monitor** *interface*
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entries.	**show running-config**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

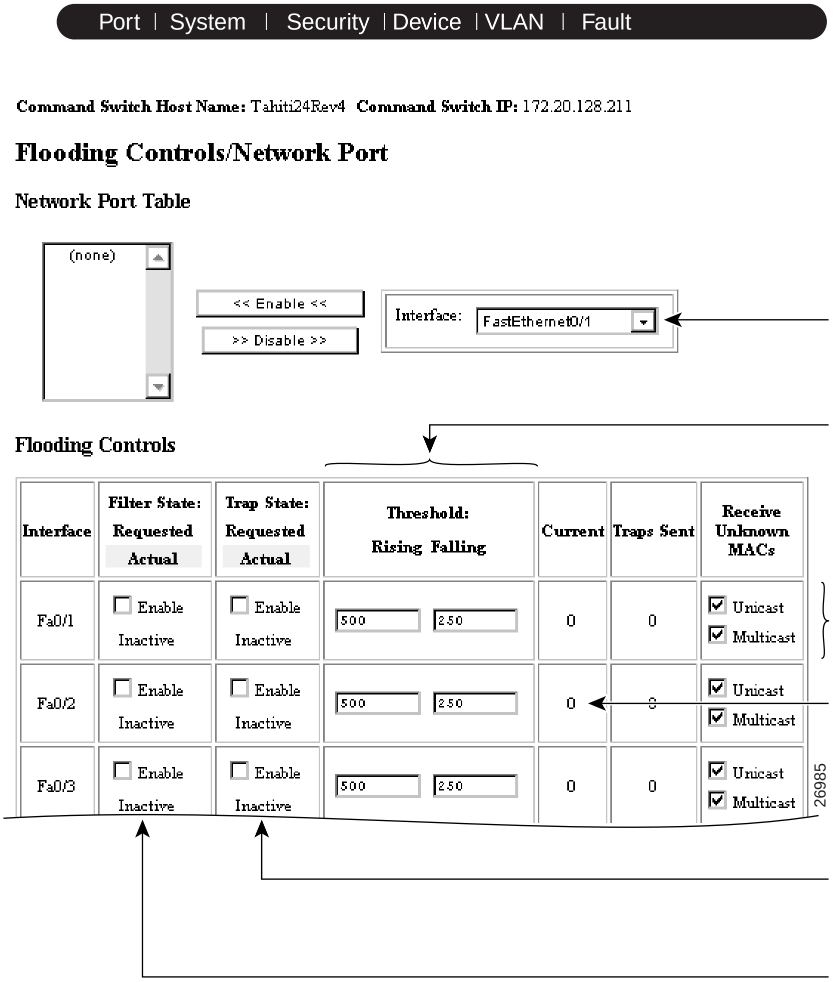
Configuring Flooding Controls

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

- 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



Command Switch Host Name: Tahiti24Rev4 **Command Switch IP:** 172.20.128.211

Flooding Controls/Network Port

Network Port Table

(none)

<< Enable <<

>> Disable >>

Interface: FastEthernet0/1

Flooding Controls

Interface	Filter State: Requested Actual	Trap State: Requested Actual	Threshold: Rising	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.

Enter 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. You can assign only one network port per VLAN.

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

For restrictions that apply to a network port, see the "Managing Configuration Conflicts" section on page 3-7.

CLI Procedure for Enabling a Network Port

Beginning in privileged EXEC mode, follow these steps 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 these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

CLI Procedure for Disabling a Network Port

Beginning in privileged EXEC mode, follow these steps to disable 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	Disable the port as the network port.	**no port network**
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entry.	**show running-config**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

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. The rising threshold is the number of broadcast packets that a switch port can receive before forwarding is blocked. The falling threshold reenables the normal 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 Procedure 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. Make sure the rising threshold is greater than the falling threshold.	**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*]

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0) documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

CLI Procedure for Disabling Broadcast Storm Control

Beginning in privileged EXEC mode, follow these steps to disable 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	Disable port storm control.	**no port storm-control**
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entries.	**show port storm-control** [*interface*]

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0) documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

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.

CLI Procedure 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 these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0) documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

CLI Procedure for Resuming Normal Forwarding on a Port

Beginning in privileged EXEC mode, follow these steps to resume normal forwarding on 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	Enable multicast forwarding to the port.	**no port block multicast**
Step 4	Enable unicast flooding to the port.	**no port block unicast**
Step 5	Return to privileged EXEC mode	**end**

Task		Command
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 these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0) documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

Reloading and Upgrading the Switch Software

Use the System Configuration page (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 software. If your switch is part of a cluster, you can also upgrade its software with the Cluster Management application. For more information, see Chapter 4, “Managing Clusters of Switches.”

You can use this page to perform the following tasks:

- Change the baud rate for the console port.
- Save the Configuration file and restart the switch.
- Change the reload options the switch uses when it restarts.
- Upgrade the software running the switch.

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

Saving the Configuration File

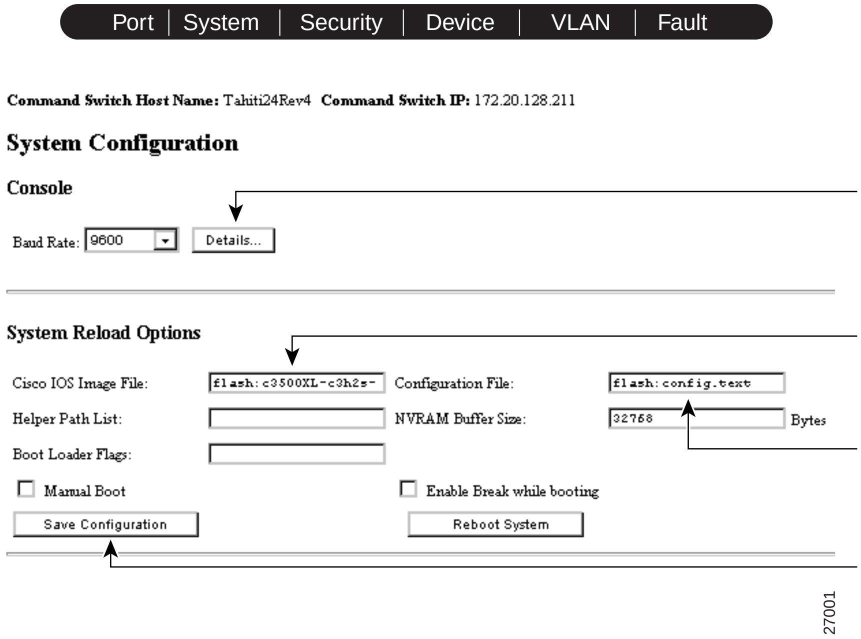
The startup configuration file (config.text) contains the IP address, passwords, and other configuration information you enter. The switch reloads this file when it restarts. However, the startup configuration file might not be the running (current) configuration. Configuration changes made through CVSM or the CLI take effect immediately on the switch 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 load the new startup configuration.

Figure 3-11 System Configuration (Part 1)



Command Switch Host Name: Tahiti24Rev4 **Command Switch IP:** 172.20.128.211

System Configuration

Console

Baud Rate: 9600

System Reload Options

Cisco IOS Image File: flash:c3500XL-c3h2s-

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 display filenames 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)
```

In the previous command display, the image file that runs the switch has a .bin extension, the html directory contains the web management application files, and config.text contains the current configuration. If you need more information about accessing the switch by using the CLI, refer to the "Configuring the Switch for Telnet" section on page 2-36.

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

Upgrading Switch Software

When you upgrade a switch, the switch continues to operate normally while the new software is copied to Flash memory. If Flash memory does not have enough space for two images, the new image is copied over the existing one. If Flash memory has enough space, the new image is copied to the selected switch but does not replace the current running image. Only after the new image is completely downloaded is the old one erased. If you experience a failure during the copy process, you can still reboot your switch using the old image. The new software is loaded the next time you reboot.

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 4-27.

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.

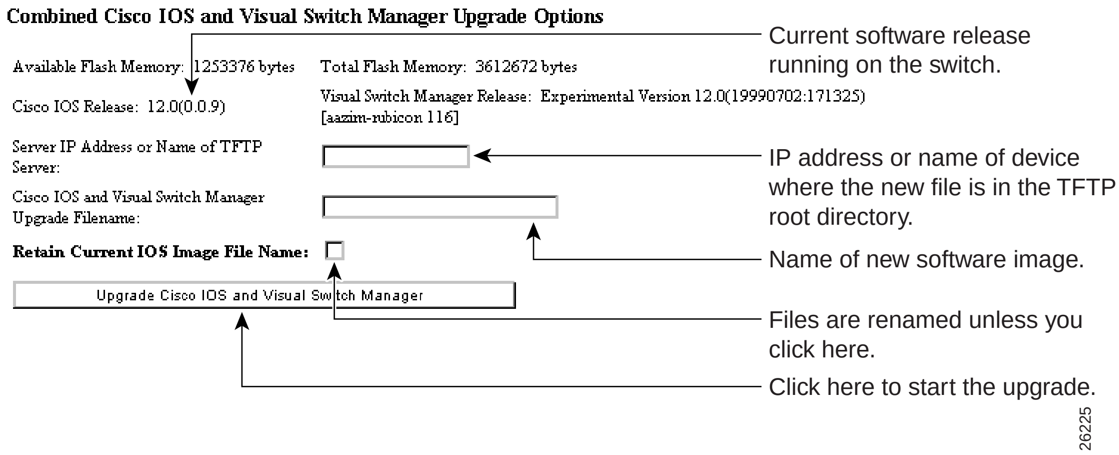
Step 2 Downloading a TFTP server if necessary.

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

Note When performing upgrades through CVSM, you can upgrade from the current release to the current release (for example, from standard to Enterprise Edition Software) or from the current release to a future release.

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

Figure 3-12 System Configuration (Part 2)



Combined Cisco IOS and Visual Switch Manager Upgrade Options

Available Flash Memory: 1253376 bytes

Total Flash Memory: 3612672 bytes

Cisco IOS Release: 12.0(0.0.9)

Visual Switch Manager Release: Experimental Version 12.0(19990702:171325) [aazim-rubicon 116]

Server IP Address or Name of TFTP Server:

Cisco IOS and Visual Switch Manager Upgrade Filename:

Retain Current IOS Image File Name: □

Current software release running on the switch.

IP address or name of device where the new file is in the TFTP root directory.

Name of new software image.

Files are renamed unless you click here.

Click here to start the upgrade.

CLI Procedure for Upgrading the Switch Software

This procedure is for switches with 8 MB of DRAM. Switches running earlier IOS releases might have less memory and require slightly different procedures. To upgrade a 2900 XL switch with 4 MB of DRAM, refer to the *Release Notes for Catalyst 2900 Series XL and Catalyst 3500 Series XL*, for Cisco IOS Release 11.2(8.1)SA6 or 11.2(8.2)SA6. These switches cannot be upgraded to IOS Release 12.0(5)XP. To determine the switch DRAM size, enter the user level **show version** command.

The upgrade procedure consists of these general steps:

- Changing the name of the *current* image file to the name of the *new* file you are copying, and replacing the old image file with the new one by using the **tar** command.
- Disabling access to the HTML pages and deleting the existing HTML files before you upgrade the software to avoid a conflict with users accessing the CVSM pages during the software upgrade.
- Reenabling access to the HTML pages after the upgrade is complete.

Beginning in privileged EXEC mode, follow these steps to upgrade the switch software:

Task		Command
Step 1	Verify that your switch has 8 MB of DRAM. For example, check the line `cisco WS-C3508G-XL (PowerPC403) processor (revision 0x01) with 8192K/1024K bytes of memory`.	**show version**
Step 2	Display the name of the current (default) image file.	**show boot**
Step 3	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.	**rename flash:***current_image* **flash:***new_image.bin*
Step 4	Display the contents of Flash memory to verify the renaming of the file.	**dir flash:**
Step 5	Enter global configuration mode.	**configure terminal**
Step 6	Disable access to the switch HTML pages.	**no IP http server**
Step 7	Return to privileged EXEC mode.	**end**
Step 8	Remove the CVSM HTML files. Press **Enter** to confirm the deletion of each file. Do not press any other keys during this process.	**delete flash:html/***
Step 9	For IOS release 11.2(8)SA5 and earlier running on 2900 XL switches, remove the files in the Snmp directory. Make sure the *S* in *Snmp* is uppercase. Press **Enter** to confirm the deletion of each file. Do not press any other keys during this process.	**delete flash:html/Snmp/***

Task		Command
Step 10	Use the **tar** command to copy the files into the switch Flash memory. Depending on the TFTP server, you might need to enter only one slash (/) after the *server_ip_address* in the **tar** command.	**tar /x tftp:**//*server_ip_address//path/filename***.tar flash:**
Step 11	Enter global configuration mode.	**configure terminal**
Step 12	Reenable access to the switch HTTP pages.	**IP http server**
Step 13	Return to privileged EXEC mode.	**end**
Step 14	Reload the new software.	**reload**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

Setting the System Date and Time

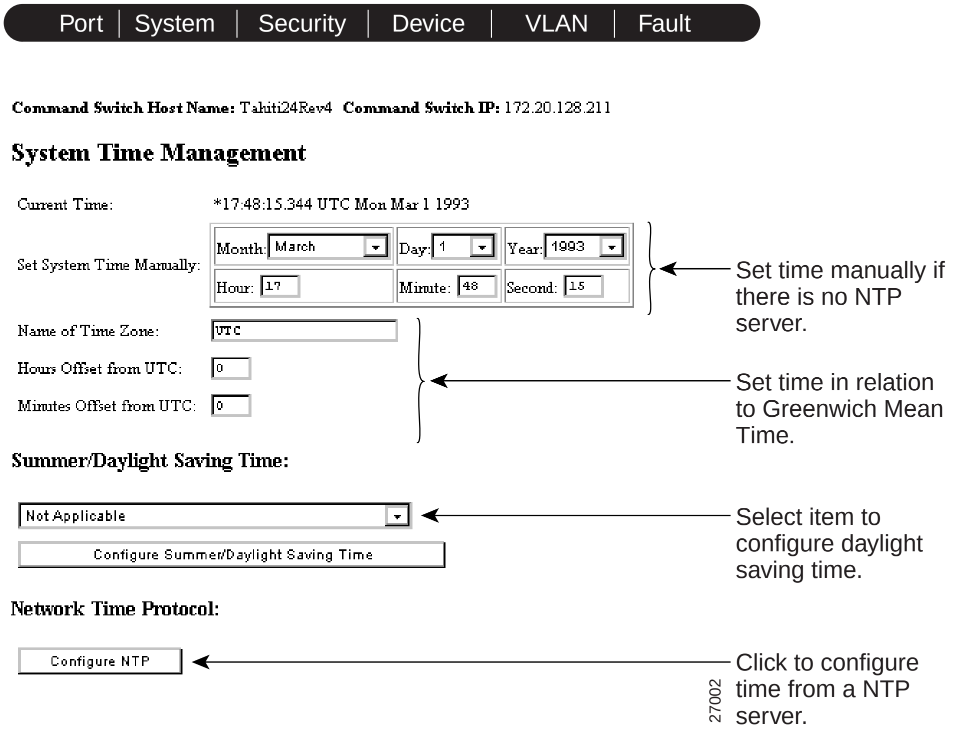
Use the System Time Management page (Figure 3-13) to set the system time for a switch or enable an external source such as Network Time Protocol (NTP) to supply time to the switch.

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



Command Switch Host Name: Tahiti24Rev4 **Command Switch IP:** 172.20.128.211

System Time Management

Current Time: *17:48:15.344 UTC Mon Mar 1 1993

Set System Time Manually:

Month: March	Day: 1	Year: 1993
Hour: 17	Minute: 48	Second: 15

Name of Time Zone: UTC

Hours Offset from UTC: 0

Minutes Offset from UTC: 0

Summer/Daylight Saving Time:

Not Applicable

Configure Summer/Daylight Saving Time

Network Time Protocol:

Configure NTP

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, such as PST for Pacific Standard Time. 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 between the switch and Greenwich, England. Enter a negative number if the switch is west of Greenwich, England, and east of the International Date Line. For example, California is eight time zones west of Greenwich, so you would enter -8 in the **Hours Offset From UTC** field. Enter a positive number if the switch is east of Greenwich. You can also enter negative and positive numbers for minutes.

To configure daylight saving time, select an option from the drop-down list, 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.

CLI Procedure for Setting the System Date and Time

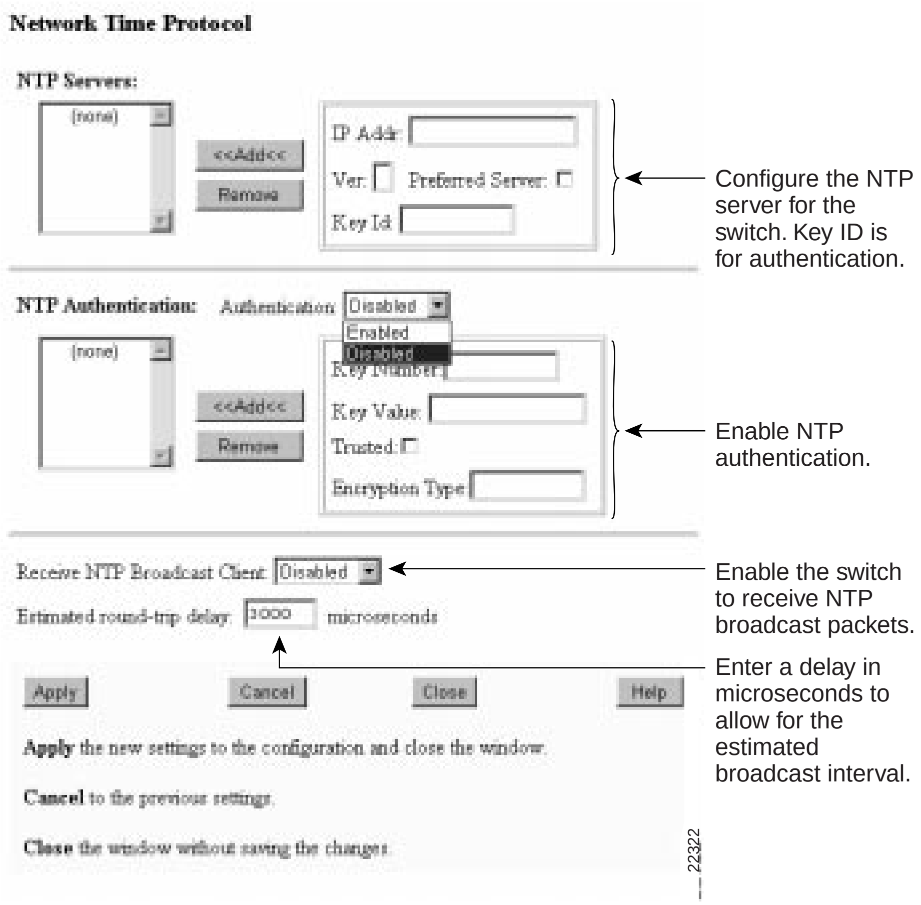
This guide describes the use of IOS commands that have been created or changed for use with switches that support IOS Release 12.0(5)XP. The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

Configuring the Network Time Protocol

In complex networks it is often prudent 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.

Figure 3-14 Network Time Protocol



Network Time Protocol

NTP Servers:

(none)

IP Addr:

Ver:

Preferred Server: □

Key Id:

NTP Authentication: Authentication: 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 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.

CLI Procedure for Configuring NTP

This guide describes the use of IOS commands that have been created or changed for use with switches that support IOS Release 12.0(5)XP. The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

Configuring IP Information

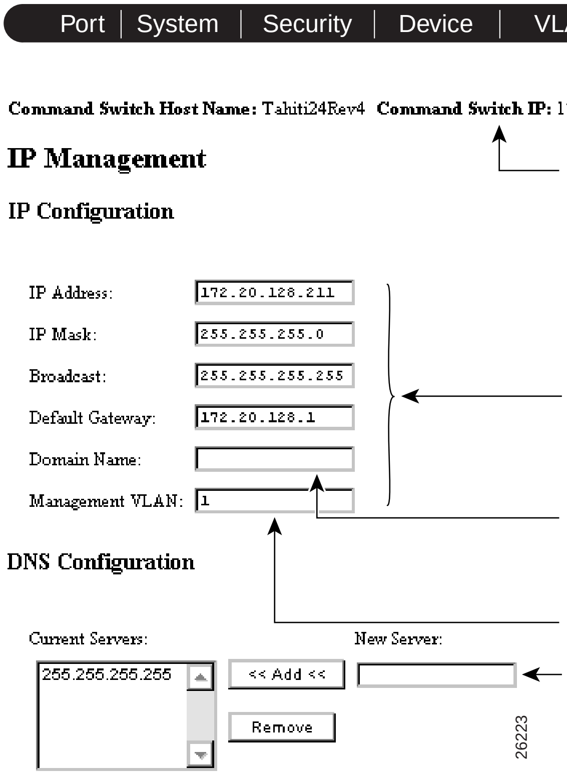
Use the IP Management page (Figure 3-15) to change or enter IP information for the switch. Some of this information, such as the IP address, you had previously entered.

You can use this page to perform the following tasks:

- Assign IP information.
- Remove an IP address.
- Configure the management VLAN interface.
- Specify a domain name, and configure the Domain Name System (DNS) server.

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

Figure 3-15 IP Management



Command Switch Host Name: Tahiti24Rev4 **Command Switch IP:** 172.20.128.211

IP Management

IP Configuration

IP Address:	172.20.128.211
IP Mask:	255.255.255.0
Broadcast:	255.255.255.255
Default Gateway:	172.20.128.1
Domain Name:	
Management VLAN:	1

DNS Configuration

Current Servers: 255.255.255.255

New Server:

Command switch defined in Cluster Builder.

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

Enter a domain name to be appended to the switch host name. Do not include the initial period. Separate a list of names with a comma and no space.

Configures the management VLAN.

Domain name servers handle name and address resolution.

Assigning IP Information to the Switch

You can use a BOOTP server to automatically assign IP information to the switch; however, the BOOTP server must be set up in advance with a database of physical MAC addresses and corresponding IP addresses, subnet masks, and default gateway addresses. In addition, the switch must be able to access the BOOTP server through one of its ports. Upon startup, a switch without an IP address requests the information from the BOOTP server; the requested information is saved in the switch running configuration file. You must log into the CLI and enter the **write memory** command to preserve this information.

You can also manually assign an IP address, mask, and default gateway to the switch through the management console. This information is required before you can access the switch using CVSM and is displayed in the IP Address, IP Mask, and Default Gateway fields of the IP Management page.

You can change the information in these fields. The mask identifies the bits that denote the network number in the IP address. When you use the mask to subnet a network, the mask is then referred to as a subnet mask. The broadcast address is reserved for sending messages to all hosts. The CPU sends traffic to an unknown IP address through the default gateway.

⚠ **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 2-8.

You can also configure the management VLAN interface and specify a domain name. For more information, see the “Configuring the Management VLAN Interface” section on page 3-54 and “Specifying a Domain Name and Configuring the DNS” section on page 3-58.

CLI Procedure 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 VLAN to which the IP information is assigned. VLAN 1 is the management VLAN, but you can configure any VLAN from IDs 1 to 1000.	**interface vlan 1**
Step 3	Enter the IP address and subnet mask.	**ip address** *ip_address subnet_mask*
Step 4	Return to global configuration mode.	**exit**
Step 5	Enter the IP address of the default router.	**ip default-gateway** *ip_address*
Step 6	Return to privileged EXEC mode.	**end**
Step 7	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 these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

CLI Procedure for Removing an IP Address

Beginning in privileged EXEC mode, follow these steps to remove an IP address:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the VLAN to which the IP information is assigned. VLAN 1 is the switch interface.	**interface vlan 1**
Step 3	Remove the IP address and subnet mask.	**no ip address** *ip_address subnet_mask*
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify that the information was removed by displaying the running configuration.	**show running-config**

Caution If you are removing the IP address through a Telnet session, your connection to the switch will be lost.

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

Configuring the Management VLAN Interface

By default, the switch IP address belongs to VLAN 1, the default management VLAN interface. However, you can configure any VLAN to be the management VLAN. Workstations connected to ports assigned to the management VLAN can establish IP connections to the switch. These connections allow access to the CVSM and SNMP. For a static-access or multi-VLAN port to access one of these management interfaces, it must also belong to the management VLAN.

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. To manage switches in a cluster, the port connections among the command, member, and candidate switches must all be on the same VLAN as the management VLAN, which is VLAN 1 by default. To change the management VLAN on an existing cluster, use the CLI and a console connection. For more information, see the “Changing the Management VLAN on an Existing Cluster” section on page 4-4.

Caution Changing the management VLAN ends your HTTP or Telnet session. You must restart the HTTP session by entering the switch IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer), or restart your CLI session through Telnet. However, you can change the management VLAN through a console connection without interruption.

Management VLAN Characteristics

The management VLAN interface has the following characteristics:

- It is created by the CVSM or the CLI on static-access, multi-VLAN, and dynamic-access and trunk ports (Enterprise Edition Software only). You cannot create or remove the management VLAN through SNMP.
- Only one management VLAN can be administratively up (active) at a time.
- With the exception of VLAN 1, the management VLAN can be deleted.
- When created, it is administratively down.
- It is used only for IP-related protocols; it is not used for Layer 2 protocols such as CDP or STP.

Guidelines for Changing the Management VLAN

Before changing the management VLAN on your switch network, make sure you follow these guidelines:

- You must be able to move your network management station to a switch port assigned to the same VLAN as the new management VLAN.
- Connectivity through the network must exist from the network management station to all switches involved in the management VLAN change.
- The switch must already have a port assigned to the same VLAN as the management VLAN. For more information, see the “Creating and Maintaining VLANs” section on page 3-101.

CLI Procedure for Configuring the Management VLAN Interface through a Console Connection

Beginning in privileged EXEC mode, follow these steps to configure the management VLAN interface through a console connection:

Task		Command
Step 1	Follow the “Guidelines for Changing the Management VLAN” section on page 3-56.	
Step 2	Enter global configuration mode.	**configure terminal**
Step 3	Enter interface configuration mode, and enter the new management VLAN to be created.	**interface vlan** *n*
Step 4	(Optional) Enter the IP address and subnet mask for the new management VLAN if this information was not previously assigned.	**ip address** *ip_address subnet_mask*
Step 5	Shutdown the current management VLAN interface, and enable the new one. If no IP information was previously assigned, this command copies the information from the old management VLAN to the new one.	**management**
Step 6	Exit the sub-interface configuration mode.	**exit**
Step 7	Exit interface configuration mode.	**exit**

Task		Command
Step 8	Return to privileged EXEC mode.	**end**
Step 9	Verify your entries.	**show interface vlan** *n*
Step 10	(Optional) Save the running configuration to the startup configuration	**copy running-config startup-config**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

CLI Procedure for Configuring the Management VLAN Interface through a Telnet Connection

Beginning in privileged EXEC mode, follow these steps to configure the management VLAN interface through a Telnet connection:

Task		Command
Step 1	Follow the "Guidelines for Changing the Management VLAN" section on page 3-56.	
Step 2	Enter global configuration mode.	**configure terminal**
Step 3	Enter interface configuration mode, and enter the new management VLAN to be created.	**interface vlan** *n*
Step 4	(Optional) Enter the IP address and subnet mask for the new management VLAN if this information was not previously assigned.	**ip address** *ip_address subnet_mask*
Step 5	Shutdown the current management VLAN interface, and enable the new one. If no IP information was previously assigned, this command copies the information from the old management VLAN to the new one.	**management**

Note After entering the **management** command, you lose connectivity to the switch. If you have connectivity from your network management station on the new management VLAN, you can reconnect to the switch. You can save the running configuration to the startup configuration by entering the privileged EXEC mode **copy running-config startup-config** command.

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

Specifying a Domain Name and Configuring the DNS

Each unique IP address can have a host name associated with it. The IOS software maintains a cache of host name-to-address mappings for use by the EXEC mode **connect**, **telnet**, **ping**, and related Telnet support operations. This cache speeds the process of converting names to addresses.

IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that the IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, the File Transfer Protocol (FTP) system for example, is identified as *ftp.cisco.com*.

To keep track of domain names, IP has defined the concept of a name server, whose job is to hold a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the host names and then specify a name server and enable the DNS, the Internet’s global naming scheme that uniquely identifies network devices.

Specifying the Domain Name

You can specify a default domain name that the software will use to complete domain name requests. You can specify either a single domain name or a list of domain names. Any IP host name that does not contain a domain name will have the domain name you specify appended to it before being added to the host table.

To specify a domain name, enter the name into the Domain Name field, and click **OK**. Do not include the initial period that separates an unqualified name (names without a dotted-decimal domain name) from the domain name.

To specify a list of domain names, enter the names separated by a comma and no space.

Specifying a Name Server

You can specify up to six hosts that can function as a name server to supply name information for the DNS. Enter the IP address into the New Server field, and click **<<Add<<**.

Enabling the DNS

If your network devices require connectivity with devices in networks for which you do not control name assignment, you can assign device names that uniquely identify your devices within the entire internetwork. The Internet’s global naming scheme, the DNS, accomplishes this task. This service is enabled by default.

CLI Procedure for Configuring DNS

This guide describes the use of IOS commands that have been created or changed for use with switches that support IOS Release 12.0(5)XP. The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

Configuring SNMP

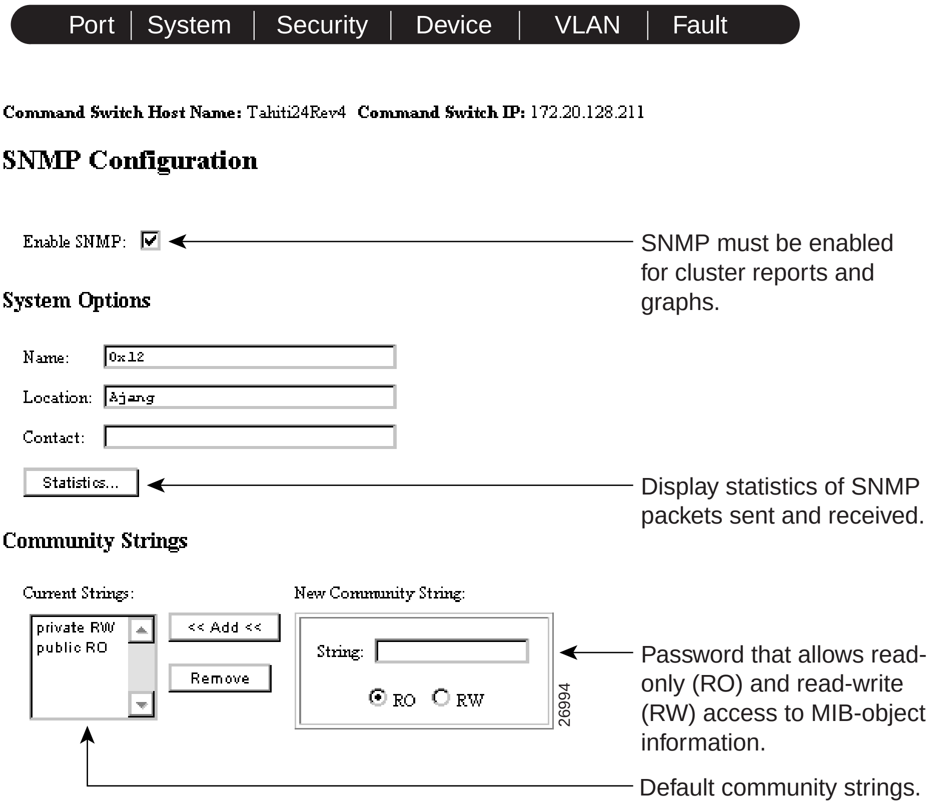
Use the SNMP Configuration page (Figure 3-16) to configure your switch for SNMP management. If your switch is part of a cluster, you can also configure SNMP with the Cluster Management application. For more information, see Chapter 4, “Managing Clusters of Switches.”

You can 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.

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

Figure 3-16 SNMP Configuration (Part 1)



Command Switch Host Name: Tahiti24Rev4 **Command Switch IP:** 172.20.128.211

SNMP Configuration

Enable SNMP: ☑

System Options

Name: 0x12

Location: Ajang

Contact:

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.

Disabling and Enabling SNMP

SNMP must be enabled for some Switch Network View and Cluster Management features to work properly. If you deselect **Enable SNMP** and click **Apply**, SNMP is disabled, and the SNMP parameters on the page disappear. For information on SNMP and Cluster Management, see “Managing Clusters through SNMP” section on page 2-41.

Entering Community Strings

Community strings serve as passwords for SNMP messages to permit access to the agent on the switch. 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.

If you are entering community strings for a cluster member, the string must be unique in the cluster.

CLI Procedure for Configuring SNMP and Community Strings

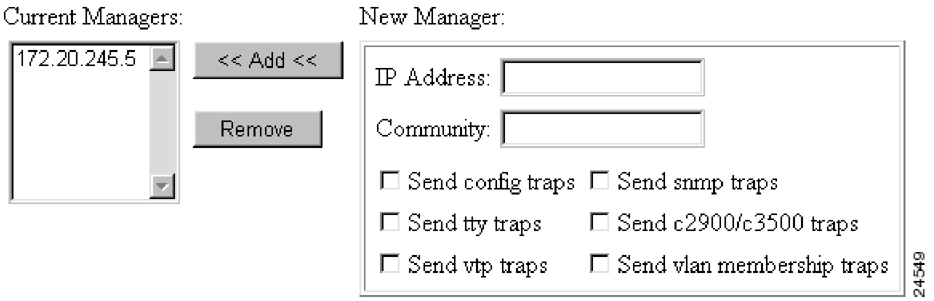
This guide describes the use of IOS commands that have been created or changed for use with switches that support IOS Release 12.0(5)XP. The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

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 by using its assigned 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

New Manager:

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 one 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 Procedure 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 these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

Managing the ARP Table

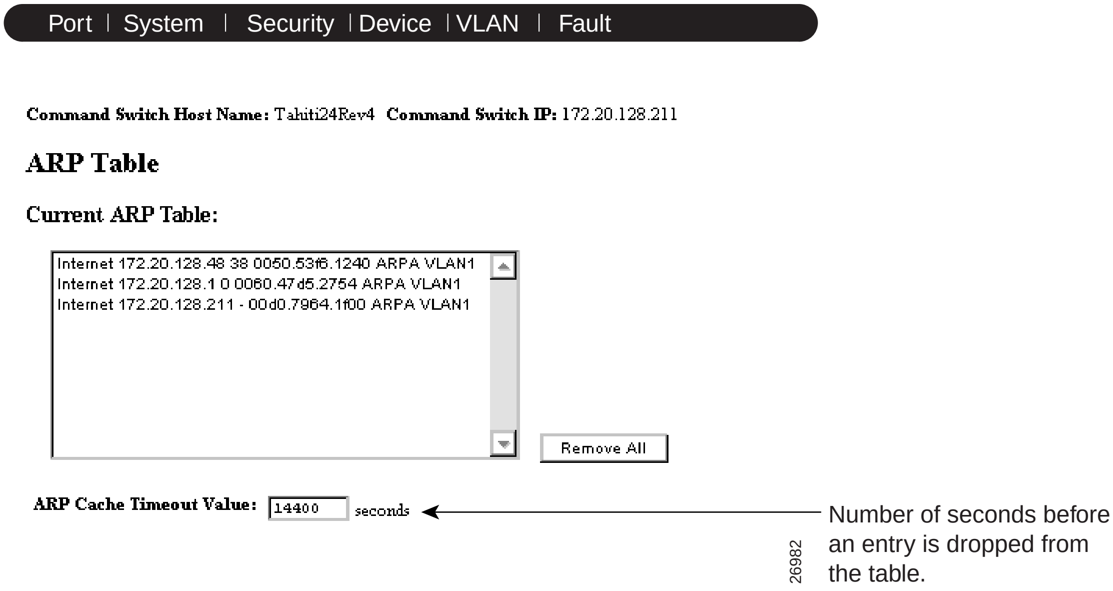
To communicate with a device (on Ethernet, for example), the software first must determine the 48-bit MAC or local data link address of that device. The process of determining the local data link address from an IP address is called *address resolution*.

The Address Resolution Protocol (ARP) is used to associate a host IP address with the corresponding media or MAC addresses and VLAN ID. Taking an IP address as input, ARP determines the associated media address. Once a media or MAC address is determined, the IP address/media address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network. Encapsulation of IP datagrams and ARP requests and replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP). By default, standard Ethernet-style ARP encapsulation (represented by the **arpa** keyword) is enabled on the IP interface.

Use the ARP Table page (Figure 3-18) to display the table and change the timeout value. 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.

Figure 3-18 ARP Table



Command Switch Host Name: Tahiti24Rev4 **Command Switch IP:** 172.20.128.211

ARP Table

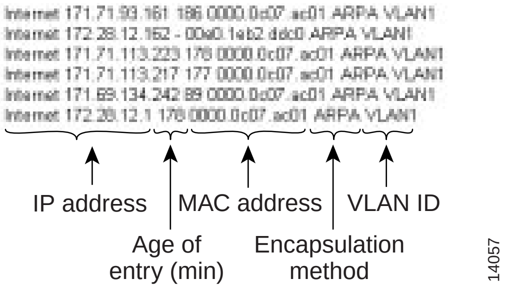
Current ARP Table:

```
Internet 172.20.128.48 38 0050.53f6.1240 ARPA VLAN1
Internet 172.20.128.1 0 0060.47d5.2754 ARPA VLAN1
Internet 172.20.128.211 - 00d0.7964.1f00 ARPA VLAN1
```

ARP Cache Timeout Value: 14400 seconds

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

Figure 3-19 Contents of the ARP Table



```
Internet 171.71.93.161 186 0000.0c07.ac01 ARPA VLAN1
Internet 172.28.12.162 - 00a0.1ab2.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
```

CLI Procedure for Managing the ARP Table

From the CLI, you can manually add entries to the ARP Table; however, these entries 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 12.0(5)XP. The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

Managing the MAC Address Tables

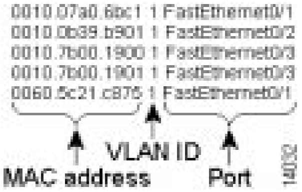
Use the Address Management page (Figure 3-21) to manage the MAC address tables that the switch uses to forward traffic between ports. These MAC tables include the following addresses:

- Dynamic address: a source MAC addresses that the switch learns and then drops when they are not in use.
- Secure address: a manually entered unicast address that specifies how packets received with the destination secure address are forwarded to a specific interface and VLAN. Secure addresses do not age.
- Static address: a manually entered unicast or multicast address that determines how frames received on a port with the destination static address are forwarded to the output ports. Static addresses do not age.

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 an example list of addresses as they would appear in the dynamic, secure, or static address table.

Figure 3-20 Contents of the Address Table



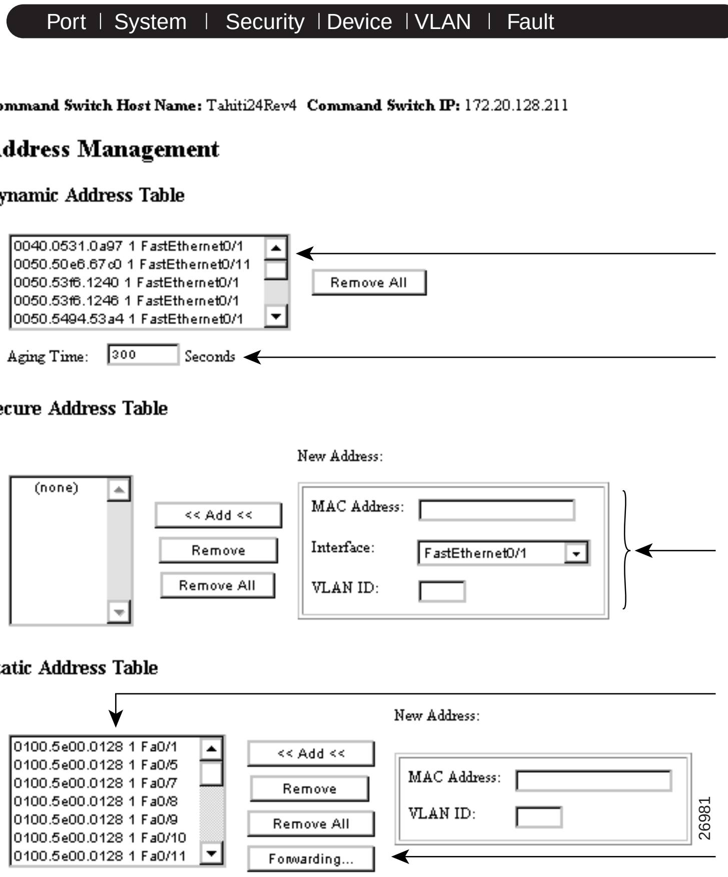
```
0010.07a0.6bc1 1 FastEthernet0/1
0010.0b39.b901 1 FastEthernet0/2
0010.7b00.1900 1 FastEthernet0/3
0010.7b00.1901 1 FastEthernet0/3
0060.5c21.c876 1 FastEthernet0/1
```

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.

Each VLAN maintains its own logical address table. 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.

Figure 3-21 Address Management



Command Switch Host Name: Tahiti24Rev4 **Command Switch IP:** 172.20.128.211

Address Management

Dynamic Address Table

```
0040.0531.0a97 1 FastEthernet0/1
0050.50e6.67c0 1 FastEthernet0/11
0050.53f6.1240 1 FastEthernet0/1
0050.53f6.1246 1 FastEthernet0/1
0050.5494.53a4 1 FastEthernet0/1
```

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 Fa0/5
0100.5e00.0128 1 Fa0/7
0100.5e00.0128 1 Fa0/8
0100.5e00.0128 1 Fa0/9
0100.5e00.0128 1 Fa0/10
0100.5e00.0128 1 Fa0/11
```

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 Procedure for Configuring the Aging Time

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

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**

Note Setting too short an aging time can cause addresses to be prematurely removed from the table. Then when the switch receives a packet for an unknown destination, it floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can impact performance. Setting too long an aging time can cause the address table to be filled with unused addresses; it can cause delays when a workstation is moved to a new port.

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

CLI Procedure for Removing Dynamic Address Entries

Beginning in privileged EXEC mode, follow these steps to remove a dynamic address entry:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter the MAC address to be removed from dynamic MAC address table.	**no mac-address-table dynamic** *hw-addr*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show mac-address-table**

You can remove all dynamic entries by using the **clear mac-address-table dynamic** command in privileged EXEC mode.

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

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 Procedure for Adding Secure Addresses

Beginning in privileged EXEC mode, follow these steps to add 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**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

CLI Procedure for Removing Secure Addresses

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

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter the secure MAC address, its associated port, and the VLAN ID to be removed.	**no mac-address-table secure** *hw-addr* **vlan** *vlan-id*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show mac-address-table secure**

You can remove all secure addresses by using the **clear mac-address-table secure** command in privileged EXEC mode.

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

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 add a static address and click **Forwarding**. On the Static Address Forwarding map, you determine how a port that receives a frame forwards it to another port for transmission. 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.

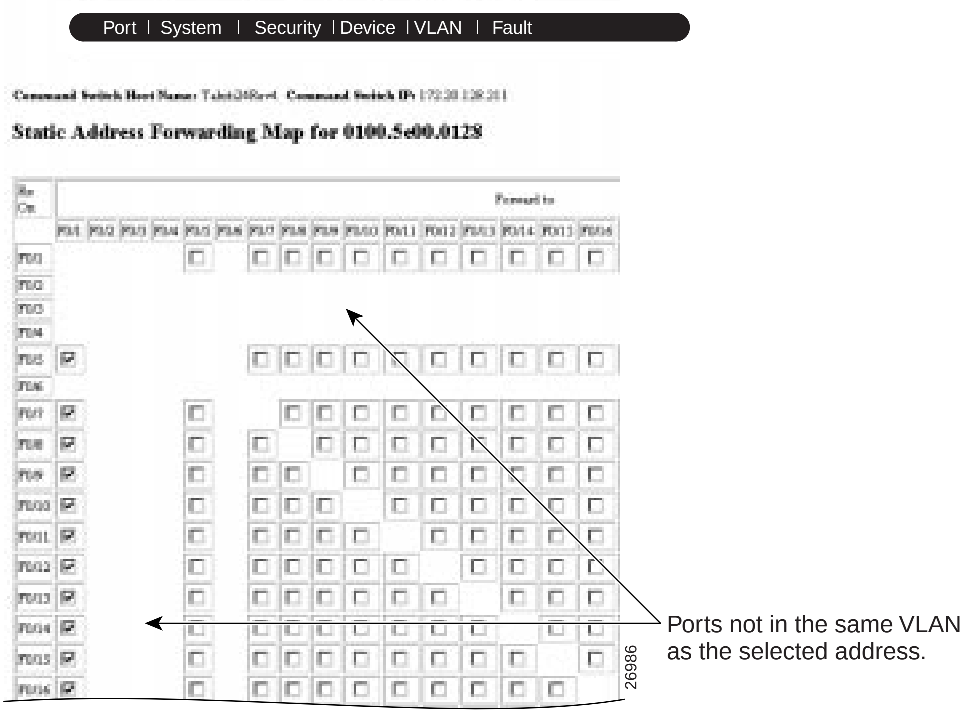
The Rx On column on the left lists the source ports. The Forward to columns lists the destination ports. Ports without check boxes belong to VLANs that a source port cannot access.

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



Command Switch Host Name: Tahiti24Rev4 **Command Switch IP:** 172.20.128.211

Static Address Forwarding Map for 0100.5e00.0128

Rx Cn	Forward to															
	Fa0/1	Fa0/2	Fa0/3	Fa0/4	Fa0/5	Fa0/6	Fa0/7	Fa0/8	Fa0/9	Fa0/10	Fa0/11	Fa0/12	Fa0/13	Fa0/14	Fa0/15	Fa0/16
Fa0/1					□		□	□	□	□	□	□	□	□	□	□
Fa0/2																
Fa0/3																
Fa0/4																
Fa0/5	☑						□	□	□	□	□	□	□	□	□	□
Fa0/6																
Fa0/7	☑				□			□	□	□	□	□	□	□	□	□
Fa0/8	☑				□		□		□	□	□	□	□	□	□	□
Fa0/9	☑				□		□	□		□	□	□	□	□	□	□
Fa0/10	☑				□		□	□	□		□	□	□	□	□	□
Fa0/11	☑				□		□	□	□	□		□	□	□	□	□
Fa0/12	☑				□		□	□	□	□	□		□	□	□	□
Fa0/13	☑				□		□	□	□	□	□	□		□	□	□
Fa0/14	☑				□		□	□	□	□	□	□	□		□	□
Fa0/15	☑				□		□	□	□	□	□	□	□	□		□
Fa0/16	☑				□		□	□	□	□	□	□	□	□	□	

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 Procedure for Adding Static Addresses

Static addresses are entered in the address table with an *in-port-list*, an *out-port-list*, and a VLAN ID, if needed. 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 ID. 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 add 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 these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

CLI Procedure for Removing Static Addresses

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

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter the static MAC address, the input port, the ports to which it can be forwarded, and the VLAN ID to be removed.	**no mac-address-table static** *hw-addr* **in-port** *in-port* **out-port-list** *out-port-list* **vlan** *vlan-id*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show mac-address-table static**

You can remove all secure addresses by using the **clear mac-address-table static** command in privileged EXEC mode.

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

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 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.

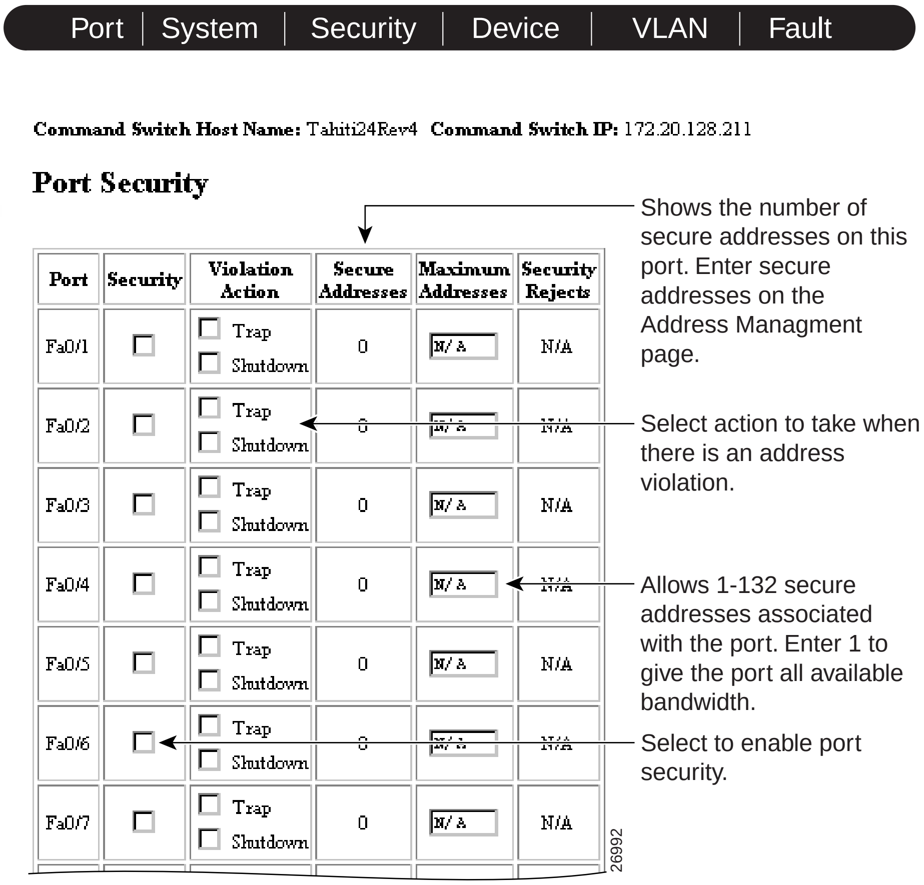
The following fields validate port security or indicate security violations:

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.

For the restrictions that apply to secure ports, see the “Managing Configuration Conflicts” section on page 3-7.

Figure 3-23 Port Security



Command Switch Host Name: Tahiti24Rev4 **Command Switch IP:** 172.20.128.211

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

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 one address in the MAC address table for the port ensures the attached device has the full bandwidth of the port.

CLI Procedure for Enabling Port Security

Beginning 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 action shutdown**
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify the entry.	**show port security**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

CLI Procedure for Disabling Port Security

Beginning in privileged EXEC mode, follow these steps to disable port security.

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode for the port you want to unsecure.	**interface** *interface*
Step 3	Disable port security	**no port security**
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify the entry	**show port security**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

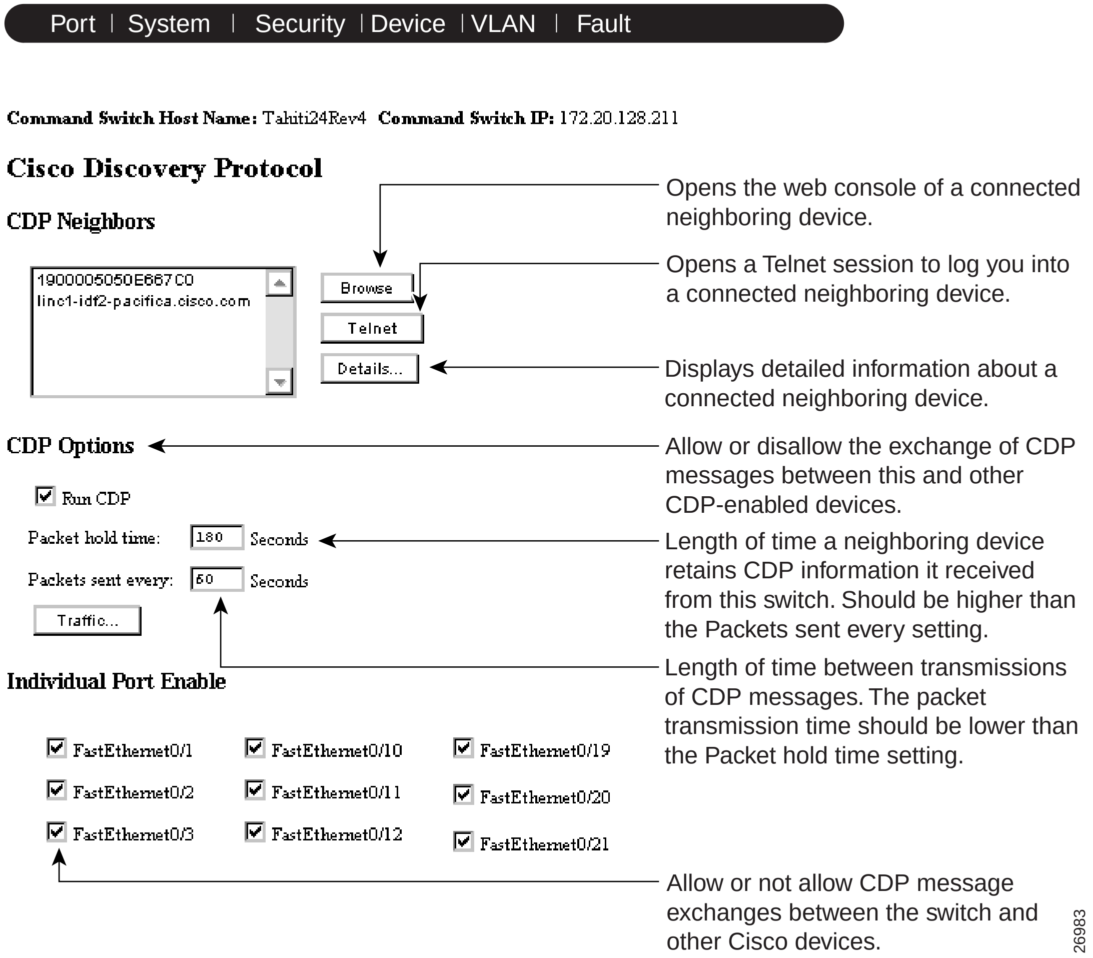
Configuring the Cisco Discovery Protocol

Use the Cisco Discovery Protocol (CDP) page (Figure 3-24) 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 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 Switch Network View and Cluster Builder.

Note Creating and maintaining switch clusters is based on the regular exchange of CDP messages. Disabling 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, select **Device>Cisco Discovery Protocol** from the menu bar.

Figure 3-24 Cisco Discovery Protocol



Command Switch Host Name: Tahiti24Rev4 **Command Switch IP:** 172.20.128.211

Cisco Discovery Protocol

CDP Neighbors

1900005050E667C0
linc1-idf2-pacifica.cisco.com

CDP Options

☑ Run CDP

Packet hold time: 180 Seconds

Packets sent every: 60 Seconds

Individual Port Enable

☑ FastEthernet0/1 ☑ FastEthernet0/10 ☑ FastEthernet0/19
☑ FastEthernet0/2 ☑ FastEthernet0/11 ☑ FastEthernet0/20
☑ FastEthernet0/3 ☑ FastEthernet0/12 ☑ FastEthernet0/21

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 Packets sent every setting.

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

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

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 by using 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 check box, you disable CDP for the entire switch and changes in the Individual Port Enable section have no effect.

- Disabling CDP on individual ports

CLI Procedure 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 12.0(5)XP. The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

Controlling IP Management Packets through CGMP

Use the Cisco Group Management Protocol (CGMP) page (Figure 3-25) to enable CGMP and the CGMP Fast Leave feature. 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 feature accelerates the removal of unused CGMP groups. By default, CGMP is enabled, and the Fast Leave feature is disabled.

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 by connected routers through the further exchange of CGMP messages.

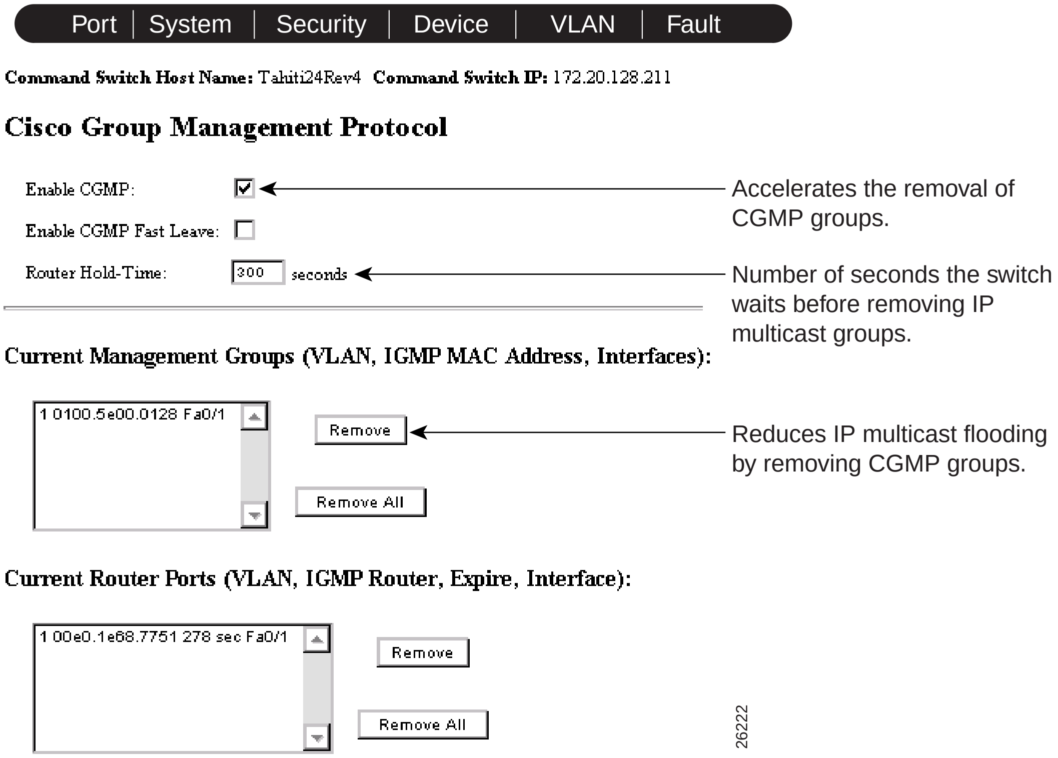
CGMP groups are maintained by VLAN: a multicast IP address packet can be forwarded to one list of ports in one VLAN and to a different list of ports in another VLAN. When a CGMP group is added, it is added on a per-VLAN, per-group basis. When a CGMP group is removed, it is only removed in a given VLAN.

You can use this page to perform the following tasks:

- Disable CGMP
- Enable the Fast Leave feature
- Remove multicast groups

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

Figure 3-25 Cisco Group Management Protocol



Command Switch Host Name: Tahiti24Rev4 **Command Switch IP:** 172.20.128.211

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 Fa0/1

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

1 00e0.1e68.7751 278 sec Fa0/1

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.

Enabling the Fast Leave Feature

The CGMP Fast Leave feature 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 feature enabled, the switch immediately checks if there are other members attached to its ports in 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.

The Fast Leave feature functions only if CGMP is enabled. The client must be running IGMP version 2 for the Fast Leave feature to function properly.

CLI Procedure for Enabling the CGMP Fast Leave Feature

Beginning in privileged EXEC mode, follow these steps to enable the CGMP Fast Leave feature:

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**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

CLI Procedure for Disabling the CGMP Fast Leave Feature

Beginning in privileged EXEC mode, follow these steps to disable the CGMP Fast Leave feature:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Disable CGMP and CGMP Fast Leave.	**no cgmp leave-processing**
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show running-config**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

Changing 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 Procedure 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**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

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 Procedure 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 all VLANs on the switch.	**clear cgmp group**
Step 2	Verify your entry by displaying CGMP information.	**show cgmp**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

Configuring the 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.

You can use this page to perform the following tasks:

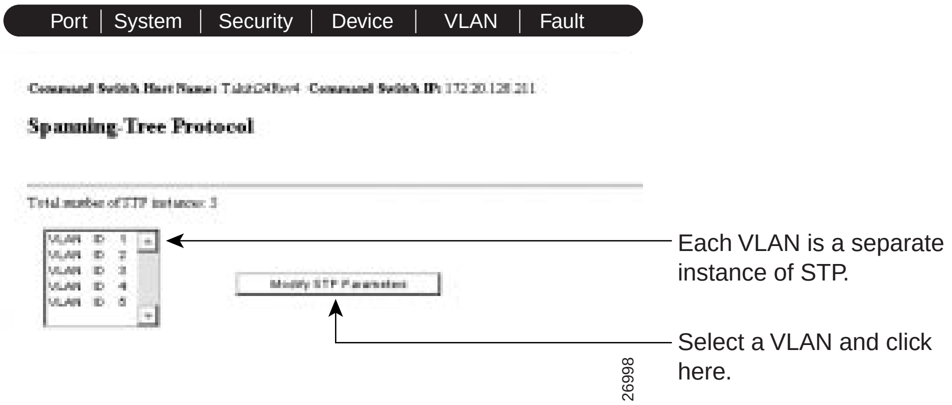
- Disable STP.
- Change STP parameters for per VLAN (STP implementation, switch priority, BPDU message interval, hello BPDU interval, and the forwarding time).
- Change STP port parameters per VLAN (Port Fast feature, path cost, port priority).

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.

Figure 3-26 Spanning-Tree Protocol (Selection)



Command Switch Host Name: Tahit24Rev4 Command Switch IP: 172.20.128.211

Spanning-Tree Protocol

Total number of STP instances: 3

VLAN ID 1
VLAN ID 2
VLAN ID 3
VLAN ID 4
VLAN ID 5

Each VLAN is a separate instance of STP.

Select a VLAN and click here.

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. For more information on creating port groups, see the "Creating EtherChannel Port Groups" section on page 3-26.

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 during a reconfiguration, 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.

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.

CLI Procedure for Disabling STP Protocol

Beginning in privileged EXEC mode, follow these steps to disable STP protocol:

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Disable STP on a VLAN.	**no spanning-tree vlan** *stp-list*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show spanning-tree**

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 remaining parameters show the other STP settings for the root switch. The root switch is the switch with the highest priority and transmits topology frames to other switches in the spanning tree.

The parameters under the heading Spanning-Tree Options are the values that this switch would use as the root switch. The following fields (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 switch. The switch 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 switch waits without receiving STP configuration messages before attempting a reconfiguration. This parameter takes effect when a switch is operating as the root switch. Switches not acting as the root use the root-switch Max age parameter.

Enter a number from 6 to 200.

Hello Time

Number of seconds between the transmission of hello messages, which indicate that the switch is active. Switches not acting as a root switch use the root-switch Hello-time value.

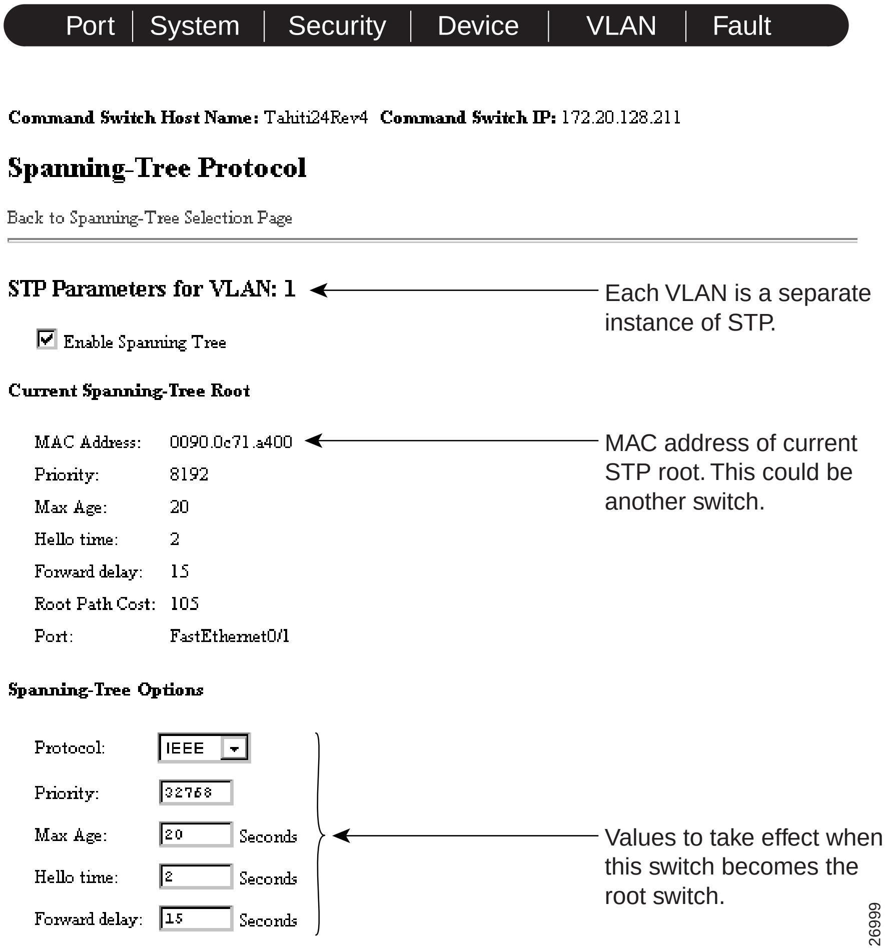
Enter a number from 1 to 10.

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)



Command Switch Host Name: Tahiti24Rev4 **Command Switch IP:** 172.20.128.211

Spanning-Tree Protocol

Back to Spanning-Tree Selection Page

STP Parameters for VLAN: 1

☑ Enable Spanning Tree

Current Spanning-Tree Root

MAC Address:	0090.0c71.a400
Priority:	8192
Max Age:	20
Hello time:	2
Forward delay:	15
Root Path Cost:	105
Port:	FastEthernet0/1

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.

CLI Procedure for Changing the STP Implementation

Beginning in privileged EXEC mode, follow these steps to change the STP implementation. The *stp-list* is the list of VLANs to which the STP command applies.

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the STP implementation to be used for a spanning-tree instance.	**spanning-tree** [**vlan** *stp-list*] **protocol** {**ieee** | **dec** | **ibm**}
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show spanning-tree**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

CLI Procedure for Changing the Switch Priority

Beginning in privileged EXEC mode, follow these steps to change the switch priority and effect which switch is the root switch. The *stp-list* is the list of VLANs to which the STP command applies.

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Configure the switch priority for the specified spanning-tree instance. Enter a number from 0 to 65535; the lower the number, the more likely the switch will be chosen as the root switch.	**spanning-tree** [**vlan** *stp-list*] **priority** *bridge-priority*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show spanning-tree**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

CLI Procedure for Changing the BPDU Message Interval

Beginning in privileged EXEC mode, follow these steps to change the BPDU message interval (max age time). The *stp-list* is the list of VLANs to which the STP command applies.

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the interval between messages the spanning tree receives from the root switch. The maximum age is the number of seconds a switch waits without receiving STP configuration messages before attempting a reconfiguration. Enter a number from 6 to 200.	**spanning-tree** [**vlan** *stp-list*] **max-age** *seconds*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show spanning-tree**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

CLI Procedure for Changing the Hello BPDU Interval

Beginning in privileged EXEC mode, follow these steps to change the hello BPDU interval (hello time). The *stp-list* is the list of VLANs to which the STP command applies.

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the interval between hello BPDUs. Hello messages indicate that the switch is active. Enter a number from 1 to 10.	**spanning-tree** [**vlan** *stp-list*] **hello-time** *seconds*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show spanning-tree**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

CLI Procedure for Changing the Forwarding Delay Time

Beginning in privileged EXEC mode, follow these steps to change the forwarding delay time. The *stp-list* is the list of VLANs to which the STP command applies.

Task		Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the forwarding time for the specified spanning-tree instance. The forward delay is the number of seconds a port waits before changing from its STP learning and listening states to the forwarding state. Enter a number from 4 to 200.	**spanning-tree** [**vlan** *stp-list*] **forward-time** *seconds*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry.	**show spanning-tree**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

Changing STP Port Parameters

The ports listed on this page (Figure 3-28) belong to the VLAN selected at the top of the page.

To change STP 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 10 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.

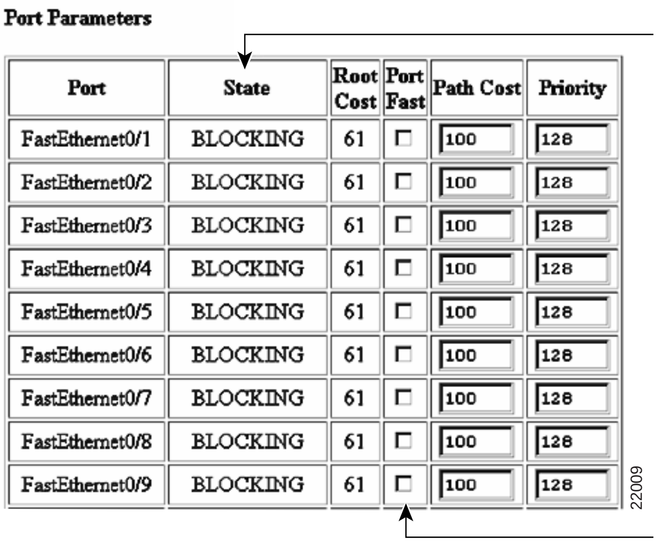
Use the following fields (Figure 3-28) to check the status of ports that are not forwarding due to STP:

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.
- Down Port has no physical link.
- Broken One end of the link is configured as an access port and the other end is configured as an 802.1Q trunk port. Or both ends of the link are configured as 802.1Q trunk ports but have different native VLAN IDs.

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.

Enabling the Port Fast Feature

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

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

CLI Procedure for Enabling STP Port Fast

Enabling this feature 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 feature:

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 these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

CLI Procedure for Changing the Path Cost

Beginning in privileged EXEC mode, follow these steps to change the path cost for STP calculations. The *stp-list* is the list of VLANs to which the STP command applies.

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	Configure the path cost for the specified spanning-tree instance. Enter a number from 1 to 65535.	**spanning-tree** [**vlan** *stp-list*] **cost** *cost*
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entry.	**show running-config**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

CLI Procedure for Changing the Port Priority

Beginning in privileged EXEC mode, follow these steps to change the port priority, which is used when two switches tie for position as the root switch. The *stp-list* is the list of VLANs to which the STP command applies.

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	Configure the port priority for a specified instance of STP. Enter a number from 0 to 255. The lower the number, the higher the priority.	**spanning-tree** [**vlan** *stp-list*] **port-priority** *port-priority*
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entry.	**show running-config**

For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

Creating and Maintaining VLANs

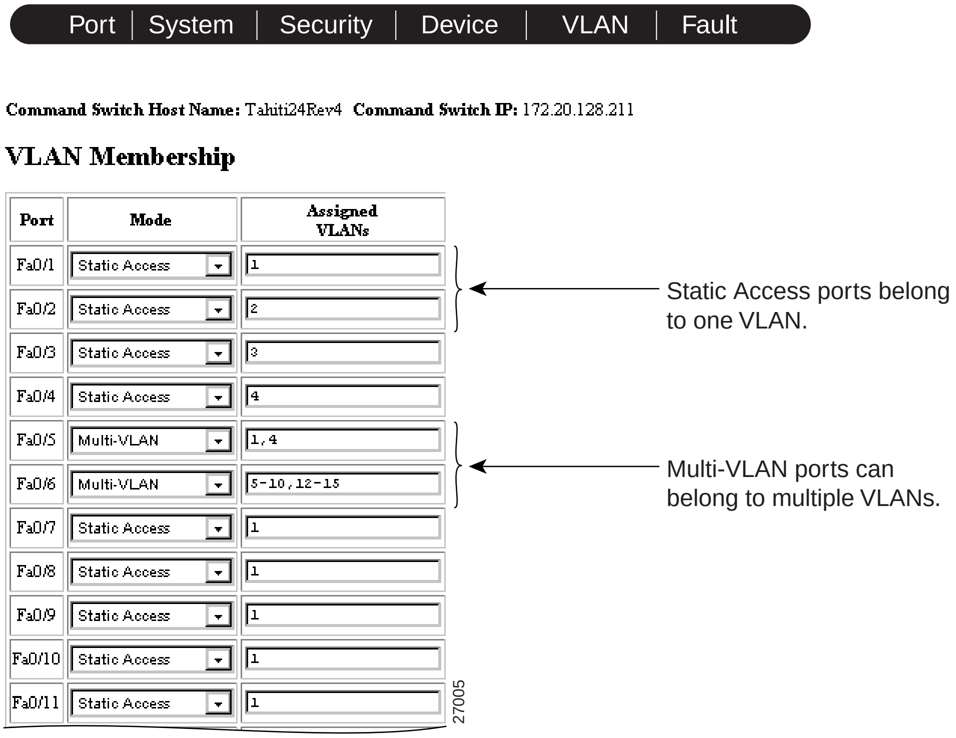
Use the VLAN Membership page (Figure 3-29) to perform the following tasks:

- Assign static-access ports to VLANs.
- Assign ports for multi-VLAN membership.

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

For the restrictions that apply to multi-VLAN ports, see the “Managing Configuration Conflicts” section on page 3-7.

Figure 3-29 VLAN Membership



Command Switch Host Name: Tahiti24Rev4 **Command Switch IP:** 172.20.128.211

VLAN Membership

Port	Mode	Assigned VLANs
Fa0/1	Static Access	1
Fa0/2	Static Access	2
Fa0/3	Static Access	3
Fa0/4	Static Access	4
Fa0/5	Multi-VLAN	1,4
Fa0/6	Multi-VLAN	5-10,12-15
Fa0/7	Static Access	1
Fa0/8	Static Access	1
Fa0/9	Static Access	1
Fa0/10	Static Access	1
Fa0/11	Static Access	1

Static Access ports belong to one VLAN.

Multi-VLAN ports can belong to multiple VLANs.

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 stations in 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).

You can configure up to 250 VLANs on all 3500 XL switches and on the following 2900 XL switches:

- WS-C2912MF-XL
- WS-C2924M-XL-A
- WS-C2924M-XL-EN

The remaining 2900 XL switches support up to 64 VLANs. Regardless of the switch model, only 64 possible instances of STP are supported.

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

Note Links among a command switch, cluster members, and candidate switches must be through ports that belong to the management VLAN interface. For more information, see the “Changing the Management VLAN on an Existing Cluster” section on page 4-4 and “Changing the Management VLAN on Candidate Switches” section on page 4-5.

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 3-67 for more information.

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.

Assigning Ports to VLANs

By default, all ports are static-access ports assigned to VLAN 1, which is the default management VLAN. The management VLAN interface is configurable and 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 management VLAN. Links among a command switch, cluster members, and candidate switches must be through ports that belong to the management VLAN interface. For information on configuring the management VLAN, see the “Configuring the Management VLAN Interface” section on page 3-54.

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 Procedure 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**

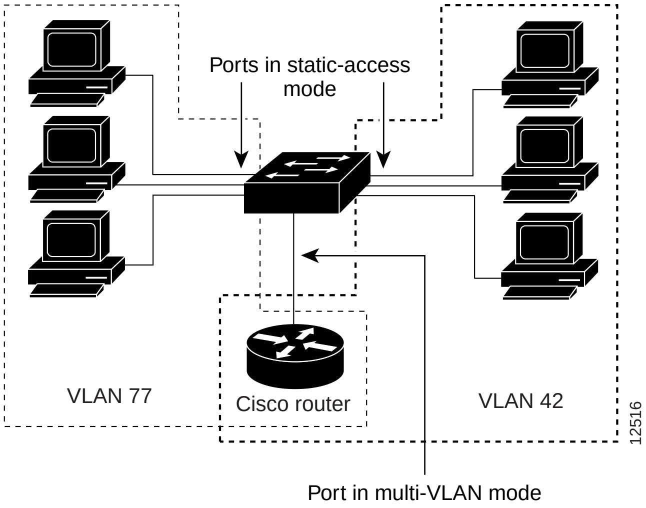
For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

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 as shown in Figure 3-30. Connectivity between VLANs is accomplished by using the router connected to the multi-VLAN port.

A multi-VLAN port performs normal switching functions 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 Procedure for Assigning Ports for Multi-VLAN Membership

Caution 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**

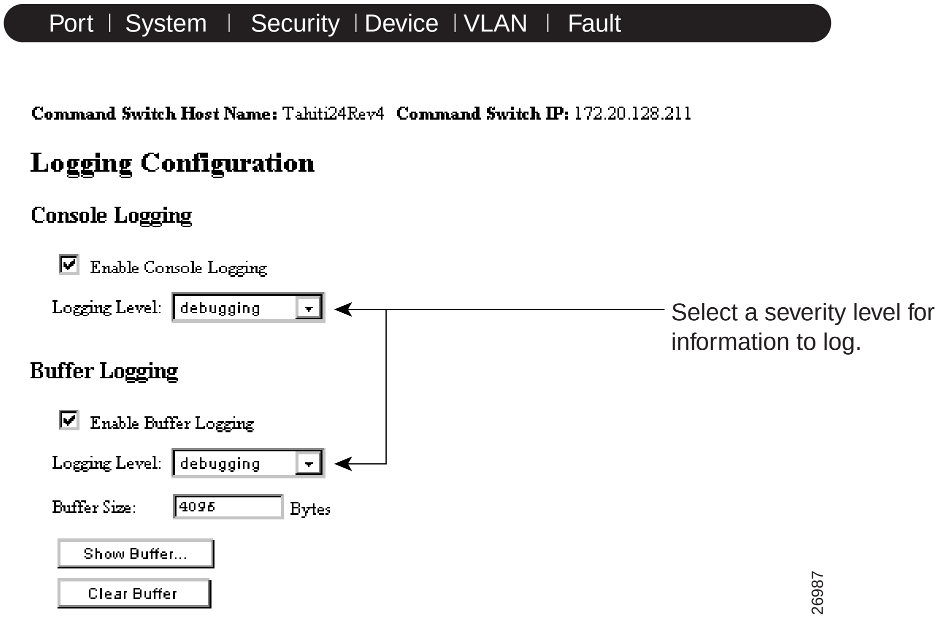
For more information on these commands, see the *Cisco IOS Desktop Switching Command Reference* (online only). The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

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.

Figure 3-31 Logging Configuration (Part 1)



Command Switch Host Name: Tahiti24Rev4 **Command Switch IP:** 172.20.128.211

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

Writes log information to the management console.

Buffer Logging

Writes 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

Maintains 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

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

Defining a Severity Level

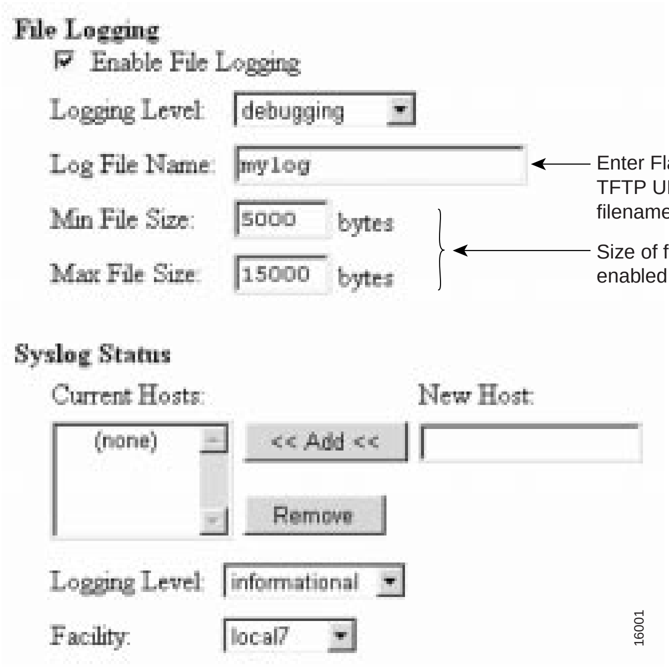
The switch can log eight levels of messages. When you select a logging level, the switch logs all syslog messages of that level and above. The default level is “Errors.” In all cases, the severity level defines the amount of detail to be logged.

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.

CLI Procedure for Configuring Logging

This guide describes the use of IOS commands that have been created or changed for use with switches that support IOS Release 12.0(5)XP. The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

Configuring the Switch for Remote Monitoring

The Remote Monitoring (RMON) feature, which is used with the SNMP agent in the switch, allows you to monitor all the traffic flowing among switches on all connected LAN segments.

You can configure your switch for RMON, which is disabled by default, by using the CLI or an SNMP-compatible network management station. You cannot configure it using CVSM. In addition, a generic RMON console application is recommended on the NMS to take advantage of RMON's network management capabilities. You must also configure SNMP on the switch to access RMON MIB objects.

RMON data is usually placed in the high-priority queue for the processor and can render the switch unusable; however, because the 2900 and 3500 XL switches use hardware counters, the monitoring is more efficient and little processing power is required.

The switch supports the following four RMON groups:

- Alarms—Allow you to monitor a specific MIB object for a specified interval, trigger an alarm at a specified value (rising threshold), and reset the alarm at another value (falling threshold). Alarms can be used with events; the alarm triggers an event, which can generate a log entry or an SNMP trap.
- Events—Allow you to determine the action to take when an event is triggered by an alarm. The action can be to generate a log entry or an SNMP trap.
- History—Allow you to collect a history group of statistics on an interface for a specified polling interval.
- Statistics—Allow you to collect Ethernet statistics on an interface.

You configure RMON alarms and events in global configuration mode by using the **rmon alarms** and **rmon events** commands. You can collect group history or group Ethernet statistics in interface configuration mode by using the **rmon collection history** or **rmon collection stats** commands.

This guide describes the use of IOS commands that have been created or changed for use with switches that support IOS Release 12.0(5)XP. The complete IOS Release 12.0 documentation is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.