

Configuring and Monitoring from the Switch Manager

This chapter explains how to use the switch manager to change the configuration settings and to monitor the switch. This chapter assumes that you have already performed these preliminary tasks that are described in this guide or in the *Quick Start Guide: Catalyst 1900 Series Ethernet Switches*:

- “Connecting to the Console Port” section on page 2-16
- “Assigning IP Information and a Password to the Switch” section on page 2-19
- “Accessing the Switch Manager” section on page 2-34

Note The switch manager online help also provides the procedures for changing the configuration settings and detailed descriptions of the fields.

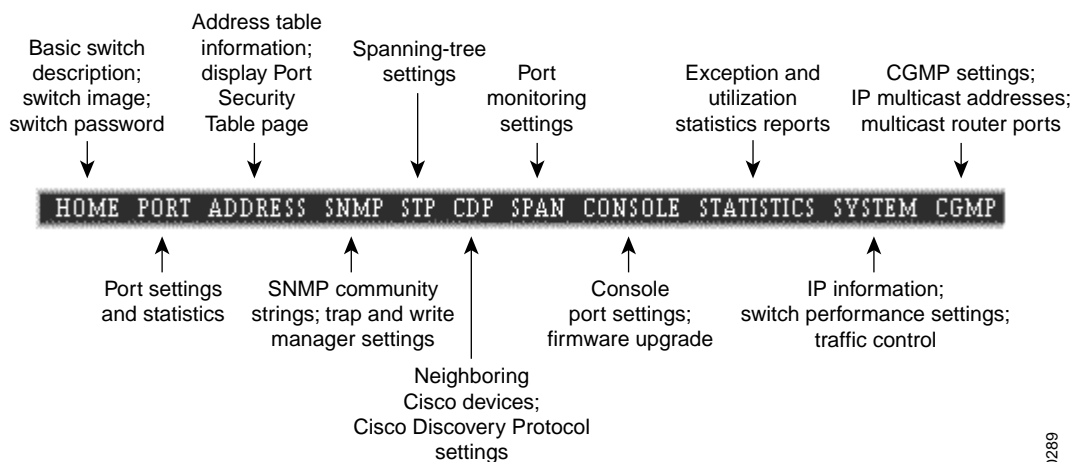
Note This chapter describes only standard-edition options. For information about the enterprise edition software features such as VLANs, see the *Catalyst 1900 Series and Catalyst 2820 Series Enterprise Edition Software Configuration Guide*.

Navigating the Switch Manager

At the top of each switch manager page is a menu bar. Figure 3-1 describes the functions of the pages accessible from this bar.

Note On Netscape Communicator, when the cursor is above a topic on the menu bar, a pop-up briefly describes the options on that particular page.

Figure 3-1 Switch Manager Menu Bar



10289

Making Changes from the Switch Manager

You can change the switch settings by entering information into fields, adding and removing list items, or selecting and deselecting check boxes. Click **Apply** to save your changes. Click **Cancel** to discard *all* your *unsaved* changes and to return the previous settings to the page.

Note After you click **Apply**, you cannot revert to the previous settings.

Note Wait approximately 1 minute for the changes to be saved to permanent storage before turning off the switch, or the changes might not be saved.

- When you enter information in fields and select or deselect check boxes, the changes are saved and take effect immediately after you click **Apply**.
- When you add items to or remove them from lists, the changes take effect immediately. It is not necessary to click **Apply**.
- If you are using Microsoft Internet Explorer 5.0 to make configuration changes to the switch, be aware that this browser does not reflect the latest configuration changes. Make sure you click the browser **Refresh** button for every configuration change.

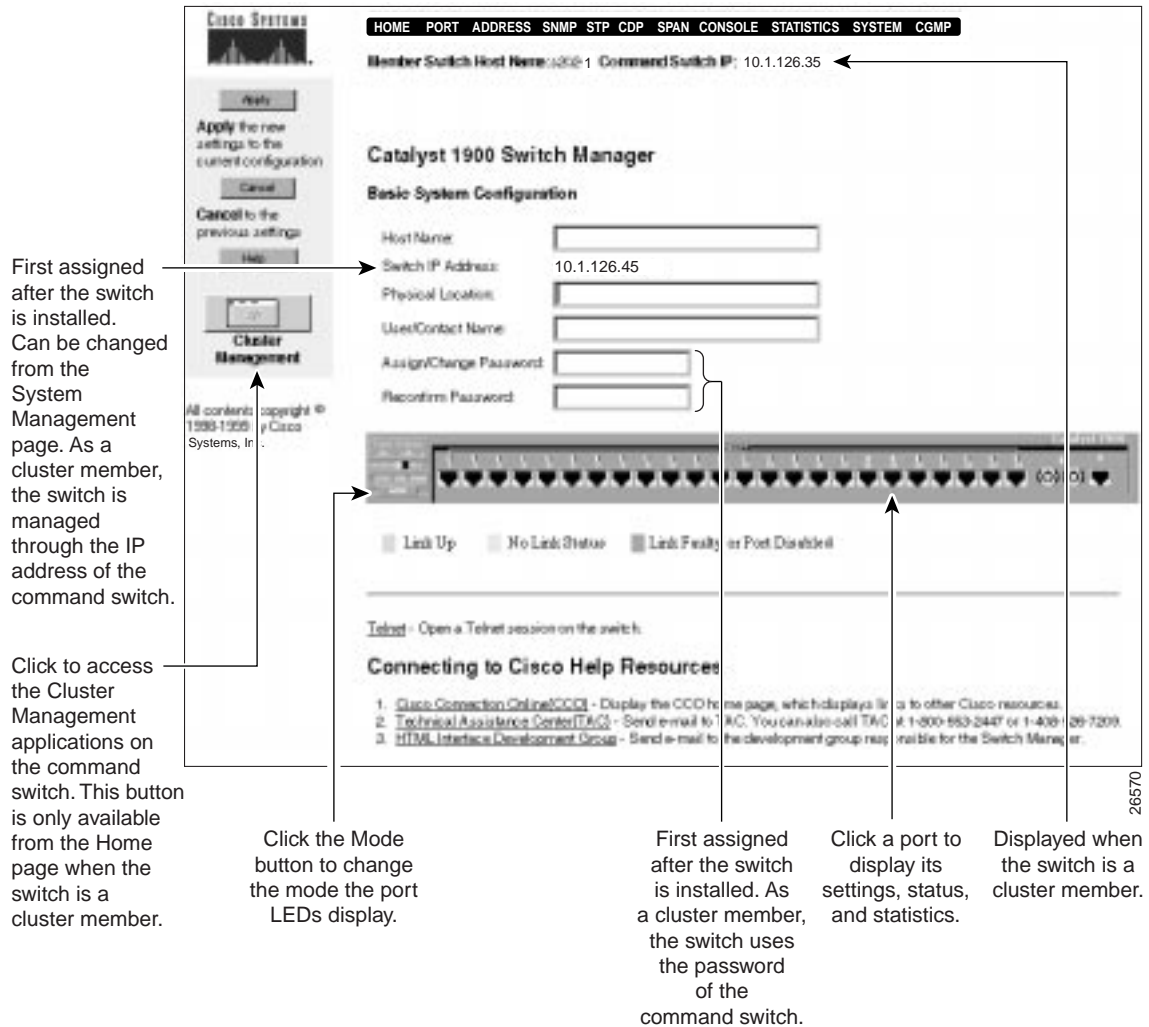
Assigning or Changing Basic Switch Information

You can assign or change basic descriptions about the switch. You can also assign an encrypted (secret) privileged-level password to the switch management interfaces and monitor network activity through the live switch image.

From the switch manager, you can open a Telnet session on the management console and contact Cisco Systems resources.

To display the Home Page (Figure 3-2), click **HOME** on the menu bar.

Figure 3-2 Home Page



Assigning or Changing the Switch Host Name and Description

You can assign or change the following information about the switch:

- Name of the switch (maximum of 255 characters)
- Physical location of the switch (maximum of 255 characters)
- Name of the person responsible for managing the switch (maximum of 255 characters)

Switch Host Name



Caution Do not use “-*NN*” (where *NN* is a number) in the name you define for the switch. When the switch joins a cluster, the command switch overwrites any name containing “-*NN*.”

The name you assign to the switch is kept even when the switch joins or leaves a cluster. If the switch does not have a name before it joins a cluster, the command switch assigns it a name that consists of the command-switch name and a number that reflects when the switch was added to the cluster. For example, a command switch can name a Catalyst 1900 switch *eng-cluster-5*, where *eng-cluster* is the command-switch name and 5 means that it is the fifth switch to join the cluster. When the switch name is viewed from the Cluster Management applications, the name is truncated to 32 characters. If the switch leaves the cluster, the switch keeps the name given by the command switch.

When the switch is a cluster member, the Member Switch Host Name field also displays the switch name at the top of each switch manager page. Therefore, the names in the Host Name and Member Switch Host Name fields are identical.

Switch and Command-Switch IP Addresses

The Switch IP Address field displays the IP address of the switch itself, which is typically assigned after the switch is installed. (See the “Assigning IP Information and a Password to the Switch” section on page 2-19.) If the switch does not have an IP address, the Switch IP Address field displays 0.0.0.0. When the switch is a cluster member, the Command Switch IP field displays the command-switch IP address at the top of each switch manager page.

IP information identifies the switch on the network and is required to configure and monitor it as an individual switch. When you assign the switch its own IP address, you can manage it from its management interfaces (switch manager, management console, SNMP, or CLI). The switch retains its own IP address even when it joins or leaves a switch cluster.

If you do not assign an IP address to the switch, you must add the switch to a switch cluster and manage it through the command switch. Whether or not the switch has its own IP address, when the switch is a cluster member, it is managed and communicates with other member switches through the IP address of the command switch. If the switch leaves the cluster and it does not have its own IP address, you then must assign IP information to it to manage and monitor it as a nonmember switch.

Note We recommend that you assign an IP address to the switch even if the switch is or will be a cluster member so that if the switch is removed from the cluster, it remains manageable as a nonmember switch.

For additional information, see the “Assigning or Changing IP Information” section on page 3-70. For information about IP information in switch clusters, refer to the *Cisco IOS Desktop Switch Software Configuration Guide, Catalyst 2900 Series XL and Catalyst 3500 Series XL Cisco IOS Release 12.0(5)XP*.

Changing the Switch Password

A privileged-level password (encrypted or unencrypted) is required to access the switch management interfaces (switch manager, management console through a Telnet session, or CLI).

The password you assign from the Assign/Change Password field on the Home Page is an encrypted (secret) privileged-level password. This password provides higher security and supersedes any existing unencrypted privileged-level password, including the unencrypted privileged-level password that is assigned from the [P] Console Password option on the Management Console Logon Screen. (For information about where you can assign privileged-level passwords, see the “Privileged-Level Passwords” section on page 3-9.)

Follow these steps to assign an encrypted privileged-level password to the switch or to change the existing switch password to an encrypted privileged-level password:

- Step 1** Enter a new password in the Assign/Change Password field. The password can be 1 to 25 characters and is *case sensitive*. You can use any character found on the keyboard, including spaces and double-quotation marks. A multistring password (such as *two words*) is also valid.
- Step 2** Reenter the same string in the Reconfirm Password field.
- Step 3** Click **Apply**.
- Step 4** Access the switch manager by using the newly assigned password.

Note When the switch is shipped, no password is assigned to it. However, a privileged-level password is required to access the Catalyst 1900 Switch Manager or to use Telnet access from a remote station. If you do not assign a password, this access will not be available until the switch joins a cluster or until you assign the switch a privileged-level password from the management console (see the “Console Settings Menu” section on page 4-6) through a direct connection to the switch console port.

When your switch is a cluster member, the highest privileged-level password for the command switch is the privileged-level password to the switch. The command-switch password overwrites any switch-specific passwords. For more information about passwords in switch clusters, see the “Cluster Member Passwords” section on page 3-10.

Note We do not recommend changing the password while the switch is a cluster member. This will cause a password mismatch, and you will have to manually enter the cluster member password to display the switch manager from the command switch.

If you have lost or forgotten the password, see the “Recovering from a Lost or Forgotten Password” section on page 5-15.

Privileged-Level Passwords

If you plan to manage the switch outside of a switch cluster, you can assign an unencrypted or encrypted privileged-level password to the switch to restrict access to its management interfaces (Table 3-1).

Table 3-1 Assigning Privileged-Level Passwords

Privileged-Level Password	Assigned from...
Unencrypted	<ul style="list-style-type: none">• [P] Console Password option on the Management Console Logon Screen• [M] Modify password option on the Console Settings Menu• CLI
Encrypted	<ul style="list-style-type: none">• Home Page• [E] Modify secret password option on the Console Settings Menu• CLI

Read and Write community strings operate as passwords to the switch when managing it from an SNMP management station. See the “Changing the SNMP Settings” section on page 3-35.

For information about the user-level passwords, refer to the online-only *Catalyst 1900 Series and Catalyst 2820 Series Command Reference*.

Cluster Member Passwords

When the switch joins a cluster, the highest privileged-level password (encrypted or unencrypted) of the command switch supersedes any existing password for the switch. Keep in mind the following considerations:

- When you add the switch to a cluster, inform other users that they must now use the command-switch password to access the switch management interfaces.
- If the command switch does not have a password, no password is required when accessing the member switch from the command switch.
- When the switch leaves the cluster, it retains the command-switch password. You can assign a different privileged-level (encrypted or unencrypted) password to the switch to manage and monitor it as a nonmember switch.

Note We do not recommend changing the password while the switch is a cluster member. This will cause a password mismatch, and you will have to manually enter the cluster member password to display the switch manager from the command switch.

For password information about switch clusters, refer to the *Cisco IOS Desktop Switch Software Configuration Guide, Catalyst 2900 Series XL and Catalyst 3500 Series XL Cisco IOS Release 12.0(5)XP*.

Using the Switch Image to Monitor the Switch

If you are using a remote station, you can use the LEDs and the Mode button on the switch image to monitor the switch. The switch image on the Home Page shows the front-panel LED colors at the last polling interval and refreshes every 30 seconds.

System Status LED on the Switch Image

The colors of the system status (SYSTEM) LED on the switch image show that the switch is receiving power and functioning properly (Table 3-2).

Table 3-2 **SYSTEM LED Description**

Color	System Status
Solid green	Switch is operating normally.
Solid amber	Switch is receiving power but might not be functioning properly. One or more power-on self-test (POST) errors occurred. The Management Console Logon Screen message identifies which nonfatal test(s) failed. Note If a fatal error occurs, the switch is not operational, and no message is displayed. (See the “Powering Up and Using POST to Test the Switch” section on page 2-6 and the “Understanding POST Failures” section on page 5-7.)

Redundant Power System LED on the Switch Image

The colors of the redundant power system (RPS) LED show the status (Table 3-3) of a connected Cisco RPS (model PWR600-AC-RPS). For more information about the RPS, see the “Power Connectors” section on page 1-12.

Table 3-3 **RPS LED Description**

Color	RPS Status
Black (off)	RPS is off or is not installed.
Solid green	RPS is operational.
Blinking green	RPS and the switch AC power supply are both powered up. Note This is not a recommended configuration. For more information, see the “Power Connectors” section on page 1-12.
Solid amber	RPS is connected but is not functioning properly. One of the power supplies in the RPS could be powered down, or a fan on the RPS could have failed.

Assigning or Changing Basic Switch Information

Port LEDs and Modes on the Switch Image

Each port has an LED above it. These LEDs, as a group or individually, display information about the switch and about individual ports (Table 3-4).

Table 3-4 Port LED Modes Summary

Mode	Determines...
Port status (default)	Status of individual ports
Bandwidth utilization	Percentage of the switch total bandwidth being used at any one time
Full-duplex operation	Which ports are operating in half- or full-duplex mode

Changing Between Modes

Click the **Mode** button on the switch image to change the mode of the port LEDs. The STAT (port status), UTL (switch utilization), and FDUP (port duplex mode) LEDs show which mode is active (Table 3-5). The selected mode remains on approximately for 30 seconds before returning to the default mode (port status). You can change the default mode from the Console Settings Menu on the management console.

Table 3-5 Changing Between Modes

For this Mode...	Push the Mode Button Until...
Port status (STAT)	Only the STAT LED is green.
Bandwidth utilization (UTL)	Only the UTL LED is green.
Full-duplex operation (FDUP)	Only the FDUP LED is green.

Port Status Mode

The port status mode is the default mode. In this mode, the colors of the LEDs above the ports show the status of those ports (Table 3-6). You cannot change the default mode from the switch manager; instead, you must use the Console Settings Menu on the management console. (See the “Console Settings Menu” section on page 4-6.)

Table 3-6 Port Status Mode LED Description

Color	Port Status
Blue (off)	No link.
Solid green	Link operational.
Alternating green and amber	Link fault. Error frames can affect connectivity. Excessive collisions, CRC errors, and alignment and jabber errors are monitored for a link-fault indication.
Solid amber	Port is not forwarding. This could be because the port was disabled by management, suspended because of an address violation, or suspended by Spanning-Tree Protocol (STP) because of network loops.

Note The LEDs are solid amber for approximately 30 seconds after power up during spanning-tree discovery.

Bandwidth Utilization Mode

In the UTL mode, the port LEDs as a group show the switch bandwidth being used at any one time. The more LEDs that are lit, the higher the bandwidth being used. The peak utilization is recorded in the bandwidth-capture interval, described in the “Bandwidth Usage Report” section on page 4-81.

Table 3-7 Bandwidth Utilization Scale with 12 and 24 10BaseT Ports

12 10BaseT Ports		24 10BaseT Ports	
Port LEDs	Mbps Activity	Port LEDs	Mbps Activity
1 to 4	0.1 to < 1.5	1 to 8	0.1 to < 6
5 to 8	1.5 to < 20	9 to 16	6 to < 120
9 to 12	20 to 140	17 to 24	120 to 280

Full-Duplex Operation Mode

The colors of the LEDs in FDUP mode show which 10BaseT and 100BaseT ports are operating in full-duplex mode (Table 3-8).

Table 3-8 FDUP LED Description

Color	Full-Duplex
Blue	Half-duplex mode is operational.
Green	Full-duplex mode is operational.

Cluster Management Button

Click **Cluster Management** to display the Cluster Management applications on the command switch. This button is available only when the switch is a cluster member. For information about the Cluster Management applications, refer to the *Cisco IOS Desktop Switch Software Configuration Guide, Catalyst 2900 Series XL and Catalyst 3500 Series XL Cisco IOS Release 12.0(5)XP*.

Link to Telnet to the Management Console

Click **Telnet** to open a Telnet session on the management console. At the prompt, enter the switch password or, if applicable, the command-switch password.

Links to Cisco Systems Resources

The Home Page provides these links to connect to Cisco Systems resources:

- Click **Cisco Connection Online (CCO)** to display the CCO home page (www.cisco.com), which contains links to the support sites for downloading the latest software and displaying the latest Cisco documentation.
- Click **Technical Assistance Center (TAC)** to send e-mail to TAC (tac@cisco.com). You can also phone TAC at 800-553-2447 or 408-526-7209.
- Click **HTML Interface Development Group** to send e-mail to the switch manager development group (cs-html@cisco.com).

Changing the Port Settings

You can change the settings of the 10- and 100-Mbps ports. To display the Port Management Page (Figure 3-3), click **PORT** on the menu bar, or click the port on the switch image.

Changing the Port Settings

Figure 3-3 Port Management Page

HOME | PORT | ADDRESS | SNMP | STP | CDP | SPAN | CONSOLE | STATISTICS | SYSTEM | CGMP

Member Switch Host Name: s202-1 Command Switch IP: 10.1.126.35

Port Management

100 Base-T Ports Table:

Module	Port	Status: Requested Actual	Duplex Mode: Requested Actual	Flood Unknown MACs	Enhanced Congestion Control	Port Name/ Description	Statistics
System	FastEthernet 0/26	<input checked="" type="checkbox"/> Enable enabled	Half duplex Half duplex	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast	Enabled		View
	FastEthernet 0/27	<input checked="" type="checkbox"/> Enable enabled	Auto-negotiate Auto-negotiate	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast	Enabled		View

10 Base-T Ports Table:

Module	Port	Status: Requested Actual	Duplex Mode: Requested Actual	Flood Unknown MACs	Port Name/ Description	Statistics
	Ethernet 0/1	<input checked="" type="checkbox"/> Enable enabled	Half duplex Half duplex	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast		View
	Ethernet 0/2	<input checked="" type="checkbox"/> Enable enabled	Half duplex Half duplex	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast		View

Set the port to use or not use ECC to help reduce congestion on the switch.

Set the port as able or unable to transmit and receive data. Displays the current port status.

Set the duplex mode of the port to half or full duplex. Displays the current duplex mode.

Set the port to forward or not forward unicast and multicast packets with unknown MAC addresses.

Displays the statistics for the port.

Use up to 60 characters to name or describe the port.

26573

Note The AUI port settings are displayed in the 10BaseT Ports Table, where the AUI port is port 13 on a 12-port switch or port 25 on a 24-port switch.

Enabling or Disabling a Port

Note You access the switch manager from a management station that is connected to one of the switch ports. Therefore, make sure that you do not disable or otherwise misconfigure the port through which you are communicating with the switch. You might want to write down the port number to which you are connected. Make changes to the switch IP information with care.

By default, all ports are enabled to transmit and receive data. To disable a port:

Step 1 Deselect the **Enable** check box in the Status: Requested/Actual column.

Step 2 Click **Apply**.

A linkDown trap is sent to the management station if you configured an SNMP manager.

Step 3 Click **Home** to display the switch image. The port LED for a disabled port is amber.

To re-enable a port:

Step 1 Select the **Enable** check box in the Status: Requested/Actual column.

Step 2 Click **Apply**.

A linkUp trap is sent to the management station if you configured an SNMP manager.

Step 3 Click **Home** to display the switch image. If the enabled port is connected to a device, the port LED is green; otherwise, it is blue.

Port Status

The Status: Requested/Actual column also displays the port status in the gray area below the **Enable** check box. Security violations, management intervention, or actions of the Spanning-Tree Protocol (STP) can change the port status. No packets are forwarded to or from a disabled or suspended port. However, suspended ports do monitor incoming packets to look for an activating condition. For example, when a linkbeat returns, a port suspended for no linkbeat returns to the enabled state.

Each port is always in one of the states listed in Table 3-9.

Table 3-9 Port Status Descriptions

Port Status	Description
Enabled	Port can transmit and receive data.
Disabled-mgmt	Port is disabled by management action. Port must be manually re-enabled.
Suspended-no-linkbeat	Port is suspended because of no linkbeat. This is usually because the attached station is disconnected or powered-down. Port automatically returns to enabled state when the condition causing the suspension is removed.
Suspended-jabber	Port is suspended because attached station is jabbering. Port automatically returns to enabled state when the condition causing the suspension is removed.
Suspended-violation	Port is suspended because of an address violation. Port automatically returns to enabled state when the condition causing the suspension is removed.
Disabled-self-test	Port is disabled because it failed a self-test.
Disabled-violation	Port is disabled because of an address violation. Port must be manually enabled.
Reset	Port is in the reset state.

Changing the Port Duplex Mode

The default duplex mode depends on the port type:

- Half duplex is the default for the 10-Mbps ports and the 100-Mbps fiber-optic ports.
- Autonegotiate is the default for the 100BaseTX ports.

To change the port duplex mode:

Step 1 Select **half duplex**, **full duplex**, **full duplex with flow control**, or **autonegotiate** from the Duplex Mode: Requested/Actual drop-down list.

The default for the 10-Mbps ports and the 100-Mbps fiber-optic ports is half duplex. The default for the 100BaseTX ports is autonegotiate.

Note The **full duplex with flow control** option is available only on the 100-Mbps ports. The **autonegotiate** option is available only on the 100BaseTX ports, not on the 10BaseT ports or the 100-Mbps fiber-optic ports.

Note After you select Auto-negotiate as the 100BaseTX port duplex mode from this page and click **Apply**, “Auto-negotiate” displays in the Actual field while the switch and the other device negotiate the duplex mode. Click **Port** on the switch manager menu bar to display the final duplex state of the port.

Step 2 Click **Apply**.

Step 3 Click **Home** to display the switch image.

Step 4 Click the **Mode** button until the FDUP LED lights. If the port LED is blue (off), the port is running in half duplex. If the port LED is green, the port is running in full duplex.

Changing the Port Settings

Full-Duplex Operation

Full-duplex operation is the simultaneous transmission of data in both directions across a link. For example, a 100-Mbps port operating in full-duplex mode can provide up to 200 Mbps of bandwidth across the switched link.

Note Both ends of the link must be configured for full-duplex operation. Because hubs operate only at half duplex, a full-duplex port on the switch cannot be connected to a hub.

Flow Control

Flow control is a function whereby the transmitting station does not send data or control information faster than the receiving station can accept it. This prevents the loss of outgoing packets during transmission. If the switch is transmitting packets faster than the attached device can receive and process them, the attached device sends pause-control frames when its port buffer becomes full. When you use the **full-duplex with flow control** option on a 100-Mbps port, the switch port responds to the pause-control frames sent from the attached device. The switch holds subsequent transmissions in the port queue for the time specified in the pause-control frame. When no more pause-control frames are received, or when the default time specified has passed, the switch resumes transmitting frames through the port.

Note Although the Catalyst 1900 switches do not generate pause-control frames, the switches do respond appropriately to pause-control frames generated by other devices.

Note Flow control on full-duplex ports is only available on the 100-Mbps ports. For information about using the **half-duplex back pressure** option on the 10-Mbps ports, see the “Half-Duplex Back Pressure on 10-Mbps Ports” section on page 3-75.

Autonegotiation

When you use the **autonegotiate** option on a 100BaseTX port, it automatically configures for full-duplex operation if the connected device also supports full duplex. If the attached device does not autonegotiate, the port automatically configures itself to half duplex.

Note Duplex negotiation is only available on the 100BaseTX ports.

Enabling or Disabling Flooding of Unknown MAC Addresses

By default, all switch ports are enabled to forward unicast and multicast packets with unknown destination Media Access Control (MAC) addresses. You can enable or disable flooding on a per-port basis.

A *unicast packet* is information addressed to one recipient from one sender. This type of traffic typically comprises the bulk of traffic on an Ethernet LAN. A *multicast packet* is information sent to multiple recipients from one sender. This lightens the load on the sender and on the network because only one data stream is sent, rather than one per recipient. A *broadcast packet* is information sent to all nodes within a single network segment and can be a major source of congestion.

The switch forwards each unicast or multicast packet it receives according to the entries stored in the switch content-addressable memory (CAM) table. The table entries are mappings of the MAC addresses of destination end-stations and of the associated switch ports through which incoming packets are forwarded to those destination end-stations.

- If the destination address is not listed in the table, the switch forwards the packet to all switch ports except the port from which the packet was received. When the destination end-station replies, the switch adds the MAC address and its associated forwarding port to the table.
- If the associated port is the same port on which the packet is received, the packet is not forwarded (filtered).

Flooding is the forwarding of unicast or multicast packets with unknown destination addresses to all the switch ports. (A broadcast packet is always forwarded [flooded] to all ports.) Flooding adds traffic on the switch ports. In some configurations, flooding could be unnecessary. For example, there are no unknown destinations on switch ports with only statically assigned addresses or single stations attached. In this case, you can disable flooding on these ports.

You can assign a network port to which all unknown unicast addresses are forwarded. For more information, see the “Network Port” section on page 3-75.

The switch can store up to 1024 address entries in memory.

For more information about address management, see the “Managing the Switch Address Tables” section on page 3-26. For information about multicast packet control, see the “Managing Multicast Packets with CGMP” section on page 3-78. For information about broadcast packet control, see the “Broadcast Storm Control” section on page 3-76.

Changing the Port Settings

To disable flooding on a port:

Step 1 Deselect the **unicast** or **multicast** check box for the port.

Step 2 Click **Apply**.

To enable flooding on a port:

Step 1 Select the **unicast** or **multicast** check box for the port.

Step 2 Click **Apply**.

Enabling or Disabling ECC on the 100-Mbps Ports

By default, enhanced congestion control (ECC) is disabled on all 100-Mbps ports. This option reduces congestion on the switch and keeps the switch from dropping frames because of full transmit queues. The ECC option can be enabled on half-duplex ports and can be configured on a per-port basis on the 100-Mbps ports.

For information about ECC on the 10-Mbps ports, see the “ECC on 10-Mbps Ports” section on page 3-76. ECC on the 10-Mbps ports is set on a global basis, not on a per-port basis.

To enable ECC on a 100-Mbps port:

Step 1 Select one of the following modes from the Enhanced Congestion Control drop-down list.

- **Adaptive**—Causes the port to operate under the ECC Disabled setting if the transmit queue is not full. If the queue is full, the port uses the ECC Aggressive setting.
- **Disabled**—Causes the port to operate under the standard IEEE 802.3 backoff algorithm for retransmitting frames.
- **Moderately Aggressive**—Causes the port to use a modified backoff algorithm to more aggressively retransmit frames and empty the queue.
- **Aggressive**—Is the highest acceleration rate configurable for ECC. The port uses a modified backoff algorithm to more aggressively retransmit frames and empty the queue than when set at ECC Moderately Aggressive.

Step 2 Click **Apply**.

Assigning or Changing a Port Name or Description

To assign a name or description to a port:

- Step 1** In the Port Name/Description column, enter the port name or a description (up to 60 characters).
- Step 2** Click **Apply**.

Detailed Port Statistics

The Detailed Port Statistics Page (Figure 3-4) displays the receive and transmit statistics for the port you select. You can use this page to help identify performance or connectivity problems, which are listed under the Errors area of the page. For example, Frame Check Sequence (FCS) and alignment errors could be the result of cabling problems such as the following:

- Cabling distance exceeded
- Split pairs
- Defective patch-panel ports
- Wrong cable type
- Misconfigured full-duplex connection

To display this page, click **View...** for a particular port on the Port Management Page. The errors are described in Table 3-10.

Changing the Port Settings

Figure 3-4 Detailed Port Statistics Page

HOME PORT ADDRESS SNMP STP CDP SPAN CONSOLE STATISTICS SYSTEM CGMP			
Member Switch Host Name: s202-1 Command Switch IP: 10.1.126.35			
Detailed Port Statistics			
Ethernet 0/1 Statistics Report			
Receive Statistics		Transmit Statistics	
Total good frames:	0	Total frames:	0
Total octets:	0	Total octets:	0
Broadcast/multicast frames:	0	Broadcast/multicast frames:	0
Broadcast/multicast octets:	0	Broadcast/multicast octets:	0
Good frames forwarded:	0	Deferrals:	0
Frames filtered:	0	Single collisions:	0
Runt frames:	0	Multiple collisions:	0
No buffer discards:	0	Excessive collisions:	0
		Queue full discards:	0
Errors:		Errors:	
FCS errors:	0	Late collisions:	0
Alignment errors:	0	Excessive deferrals:	0
Giant frames:	0	Jabber errors:	0
Address violations:	0	Other transmit errors:	0

26574

Table 3-10 **Error Descriptions**

Error	Description
FCS errors	Number of frames received on a particular interface that are an integral number of octets in length but do not pass the Frame Check Sequence (FCS) test.
Alignment errors	Number of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS test.
Giant frames	Number of frames received on a particular interface that exceed the permitted frame size.
Address violations	Number of times this secure port receives a source address that duplicates a static address configured on another port plus the number of times a source address was seen on this port that does not match any addresses secured for the port.
Late collisions	Number of times the port detects a collision on a particular interface later than 512 bit-times into the transmission of a packet.
Excessive deferrals	Number of frames the port defers transmission for an excessive period of time.
Jabber errors	Number of times the jabber function was invoked because a frame received from this port exceeded a certain time duration.

Managing the Switch Address Tables

The switches use source address tables (filters) to efficiently forward packets between the switch ports. Address filtering applies only to incoming (received) traffic on the switch. The source address tables list the source addresses (sending end-stations) and the associated switch port(s) through which packets are forwarded to the destination end-stations.

Packets with static addresses are usually received on any source port. The switch also supports source-port filtering on unicast and multicast addresses. This enhanced filtering enables the switch to only forward packets from source addresses when they are received on specified switch ports. These source addresses are referred to as *restricted static addresses*.

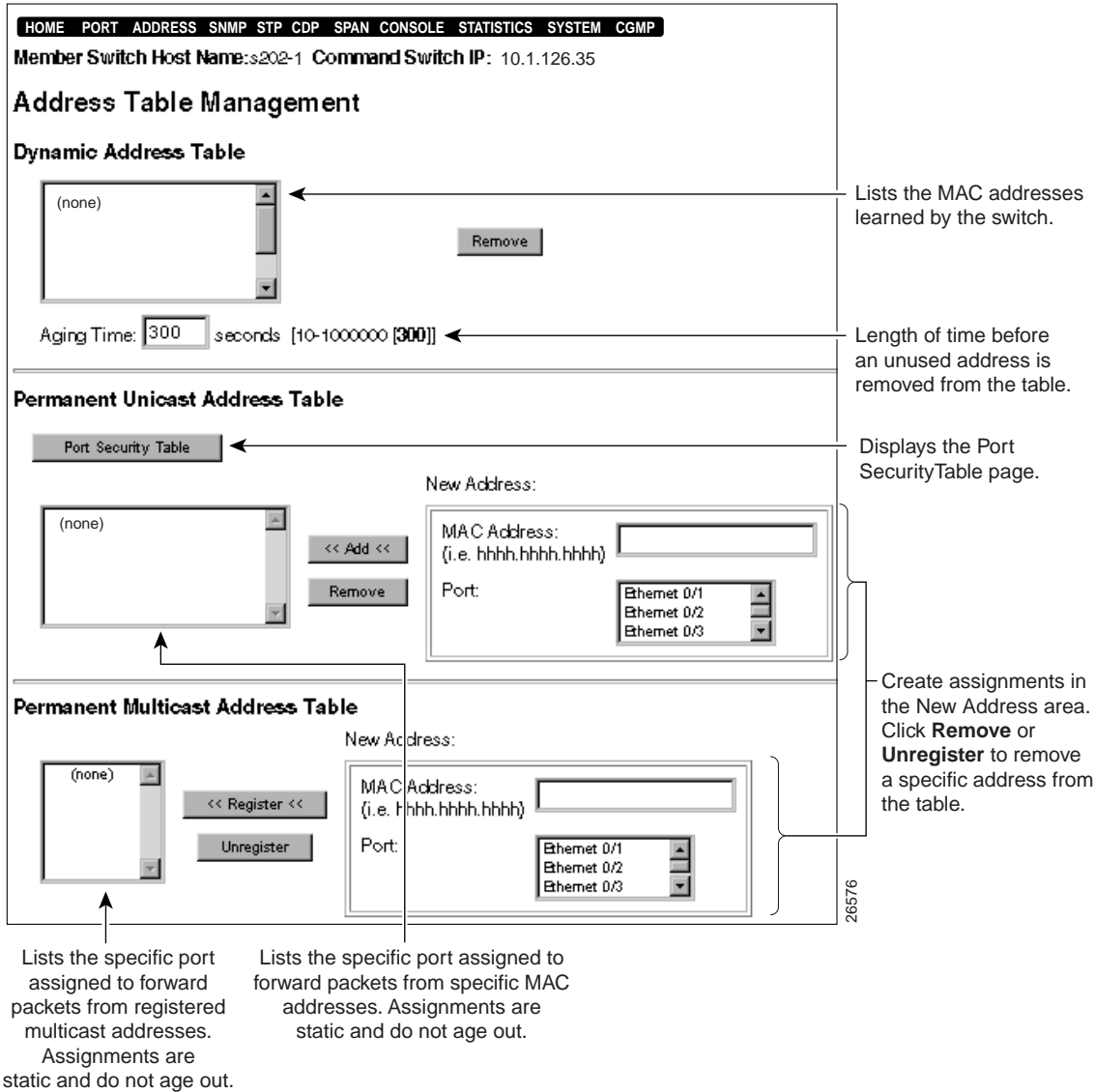
The switch can store up to 1024 address entries in memory.

For additional traffic control options, see the following sections:

- “Enabling or Disabling Flooding of Unknown MAC Addresses” section on page 3-21
- “Switch Performance and Flooding and Traffic Control” section on page 3-73
- “Broadcast Storm Control” section on page 3-76
- “Managing Multicast Packets with CGMP” section on page 3-78

To display the Address Table Management Page (Figure 3-5), click **Address** on the menu bar.

Figure 3-5 Address Table Management Page



Dynamic Address Table

The switch provides dynamic addressing by learning the source MAC address of each packet received on each switch port and then adding the address and its associated forwarding switch port number to the Dynamic Address Table. As end-stations are added or removed from the network, the switch updates the table, adding new entries and removing unused ones.

To delete a specific entry from the Dynamic Address Table:

Step 1 Select the entry you want to delete.

Step 2 Click **Remove**.

Changing the Address Aging Time

As the switch reaches the maximum address limit of 1024 address entries in memory, switch performance can degrade. Address aging helps prevent this by allowing the switch to keep only dynamic addresses that remain active over a specified period of time.

During a topology change, if the Port Fast mode option on the Port Management Page is disabled, addresses are aged more quickly by using the Forward delay option on the Spanning-Tree Management Page. When the topology stabilizes, the address-aging value again takes effect.

To assign the length of time the switch stores an inactive entry, after which it is removed from the table:

Step 1 Enter the number of seconds (10 to 1000000; where 1000000 seconds is approximately 11 1/2 days) in the Aging Time field. The default is 300 seconds (5 minutes).

This value applies to all dynamic addresses in the Dynamic Address Table.

Step 2 Click **Apply**.

Permanent Unicast Address Table

The entries in the Permanent Unicast Address Table allow MAC addresses to be permanently associated with a switch port. Unlike the Dynamic Address Table, the entries in the Permanent Unicast Address Table are manually entered or *sticky-learned*. (See the “Securing a Port” section on page 3-33.)

If the address table is full, an error message is generated. You can change the size of the address table by using the Port Security Table Page. (See the “Changing the Maximum Secure Address Count” section on page 3-33.) For additional information about port security, see the “Changing the Port Security Table” section on page 3-31.

You can assign a network port to which all unknown unicast addresses are forwarded. For more information, see the “Network Port” section on page 3-75.

Note Only unicast addresses can be added. An attempt to add a multicast or broadcast address generates an error message.

To add a secure address to the Permanent Unicast Address Table:

- Step 1** Select a switch port from the New Address scroll list.
- Step 2** Enter the source MAC address in the MAC Address field. Use six hexadecimal octets, spaces are optional (such as hh hh hh hh hh hh or hhhhhhhhhhhh).
- Step 3** Click **Add**.

Static entries do not age out and must be manually removed from the table. To delete an entry from the table:

- Step 1** Select the entry you want to delete.
- Step 2** Click **Remove**.

Permanent Multicast Address Table

The entries in the Permanent Multicast Address Table allow multicast addresses to be permanently associated with the switch port(s) that receive packets destined for those multicast addresses. Using the Permanent Multicast Address Table reduces the amount of multicast flooding on the switch. Unlike the Dynamic Address Table, the entries in the Permanent Multicast Address Table entries are manually entered.

If the address table is full, an error message is generated. You can change the size of the address table by using the Port Security Table Page. (See the “Changing the Maximum Secure Address Count” section on page 3-33.)

For additional information, see the

- “Changing the Port Security Table” section on page 3-31
- “Managing Multicast Packets with CGMP” section on page 3-78

To add a secure address to the Permanent Multicast Address Table:

Step 1 Select a switch port from the New Address scroll list.

Step 2 Enter the multicast MAC address in the MAC Address field. Use six hexadecimal octets, spaces are optional (such as hh hh hh hh hh hh or hhhhhhhhhhhh).

Step 3 Click **Register**.

Static entries do not age out and must be manually removed from the table. To delete an entry from the table:

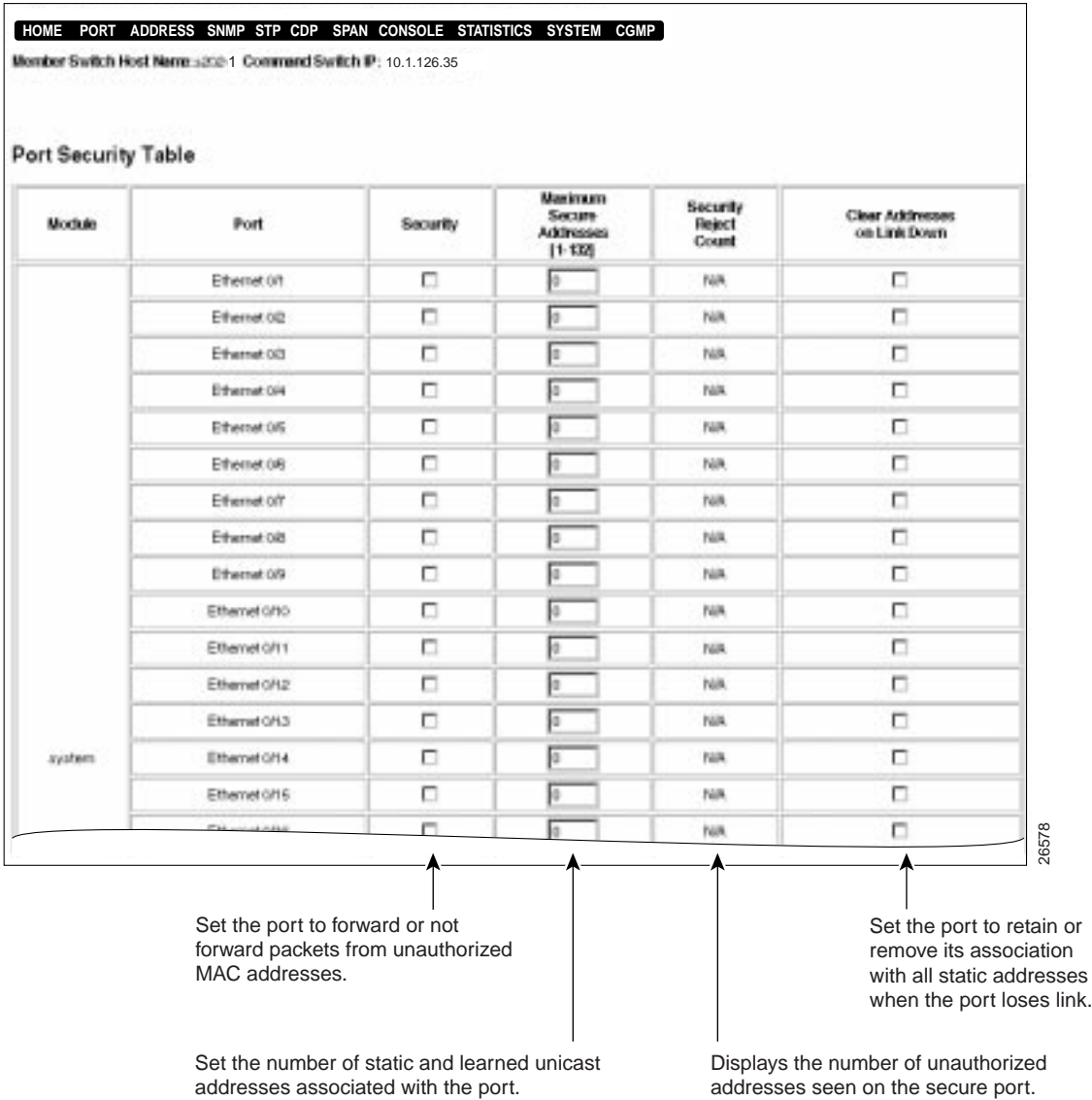
Step 1 Select the entry you want to delete.

Step 2 Click **Unregister**.

Changing the Port Security Table

You can use the Port Security Table Page (Figure 3-6) to prevent the switch from forwarding packets from unauthorized users and to send SNMP traps if security violations occur. To display this page, click **Port Security Table** from the Address Table Management Page.

Figure 3-6 Port Security Table Page



Securing a Port

By default, port security is disabled (**Security** check box is not selected). Secure ports restrict the use of a switch port to a specific group of source addresses (sending end-stations). When you assign source addresses to a secure port, the switch does not forward any packets from addresses outside that group.

The source addresses on a secure port are manually assigned (static) or *sticky-learned*. Sticky-learning takes place when the address table for a secure port does not contain a full complement of static addresses. The port sticky-learns the source address of incoming packets and automatically assigns them as static addresses.

Note This option must be disabled on the network port. For more information about the network port, see the “Network Port” section on page 3-75.

To enable port security on a port:

Step 1 Select the check box in the Security column for the port.

Step 2 Click **Apply**.

To disable port security on a port:

Step 1 Deselect the check box in the Security column for the port.

Step 2 Click **Apply**.

Changing the Maximum Secure Address Count

If the port is not a secure port, the value in the Maximum Secure Addresses field is 0. A secure port can have from 1 to 132 secure addresses associated with it.

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 10 Mbps or 100 Mbps of the port.
- **Added security**—Devices cannot connect to the port without your knowledge.

Note The size of the address table for an unsecured port cannot be modified.

Managing the Switch Address Tables

To change the number of addresses to the secure port:

Step 1 Enter a number (1 to 132) in the Maximum Secure Addresses column.

Step 2 Click **Apply**.

Security Reject Count

The Security Reject Count (SRC) column displays the number of unauthorized addresses seen on the secure port.

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

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

If a security violation occurs, the port can be suspended or disabled. When a port is disabled, you must manually re-enable the port. When a port is suspended, it is re-enabled when a packet containing a valid address is received. You can also choose to ignore the violation. You can define the action taken by the switch either by using the System Management Page or by using the MIB objects.

On the following switch manager pages, you can specify the action the switch takes if packets with unauthorized addresses arrive on the port:

- On the SNMP Management Page, you can enable or disable trap generation.
- On the System Management Page, you can assign the switch to ignore, suspend, or disable the port if an address violation occurs. (For more information, see the “Action Upon Address Violations” section on page 3-74.)

Clearing Addresses on LinkDown

By default, the secure port keeps its association with all static addresses even if it loses link (**Clear Addresses on LinkDown** check box is not selected). You can enable a secure port to clear its address associations on linkDown.

Note This option is applicable only to secure ports (**Security** check box is selected).

To enable the secure port to clear its address table on linkDown:

- Step 1** Select the check box in the Clear Addresses on LinkDown column for the port.
- Step 2** Click **Apply**.

To disable the secure port from clearing its address table on linkDown:

- Step 1** Deselect the check box in the Clear Addresses on LinkDown column for the port.
- Step 2** Click **Apply**.

Changing the SNMP Settings

Simple Network Management Protocol (SNMP) provides the means to manage and monitor the switch through the Management Information Base (MIB) objects. Additional information about SNMP and MIB objects is in the “Simple Network Management Protocol” section on page 1-24 and the “Accessing MIB Files” section on page 2-44.

For information about how the command switch uses SNMP to manage the switch in the cluster, refer to the *Cisco IOS Desktop Switch Software Configuration Guide, Catalyst 2900 Series XL and Catalyst 3500 Series XL Cisco IOS Release 12.0(5)XP*.

To display the SNMP Management Page (Figure 3-7), click **SNMP** on the menu bar.

Changing the SNMP Settings

Figure 3-7 SNMP Management Page

The screenshot displays the SNMP Management configuration page. At the top, a navigation bar includes links: HOME, PORT, ADDRESS, SNMP, STP, CDP, SPAN, CONSOLE, STATISTICS, SYSTEM, and CGMP. Below this, the page title is "SNMP Management".

Read Community Strings (maximum of 4):

Current: A list box showing "public" and "private @es". Buttons: "<< Add <<" and "Remove".

New: A "String:" label followed by a text input field.

Write Community Strings (maximum of 4):

Current: A list box showing "private" and "private @es". Buttons: "<< Add <<" and "Remove".

New: A "String:" label followed by a text input field.

Trap Managers (maximum of 4):

Current: A list box showing "(none)". Buttons: "<< Add <<" and "Remove".

New: Two text input fields labeled "IP Address/Hostname:" and "Trap Manager Community String:".

Enable Authentication Trap Generation: ☒
Enable LinkUp/LinkDown Trap Generation: ☒
Enable Broadcast Storm Trap Generation: ☐
Enable Address Violation Trap Generation: ☒

Write Managers (maximum of 4):

Current: A list box showing "(none)". Buttons: "<< Add <<" and "Remove".

New: A text input field labeled "IP Address/Hostname:".

Annotations on the right side of the form:

- Line 1: Points to the Read Community Strings "New" field. Text: "Passwords that allow read-only (Get requests) access to the switch MIB-object information. When the switch is a cluster member, the last string is from the command switch. Do not use '@es' in the strings you define."
- Line 2: Points to the Write Community Strings "New" field. Text: "Passwords that allow read-write (Get requests) access to the switch MIB-object information. When the switch is a cluster member, the last string is from the command switch. Do not use '@es' in the strings you define."
- Line 3: Points to the Trap Managers "New" fields. Text: "Management stations that can receive SNMP traps (alerts of certain events) generated by the switch. Use the traps to monitor the switch."
- Line 4: Points to the trap generation checkboxes. Text: "Set the switch to generate or not generate these types of traps."
- Line 5: Points to the Write Managers "New" field. Text: "Management stations that can issue write requests to change the switch configuration settings through the MIB variables. Available when the switch has its own IP address."

26580

Assigning or Changing the SNMP Read Community Strings

The default for the first Read community string is public. You can assign up to four community strings to serve as passwords that enable the switch to validate SNMP read (Get) requests from a management station.

When the switch joins a cluster, the command switch propagates its first Read community string as the last Read community string for the member switch. If the joining Catalyst 1900 switch already has four Read community strings, the command switch overrides that fourth community string with its own first community string. When the switch leaves the cluster, the command-switch community string is deleted.

The command-switch string contains up to 27 characters and a suffix “@es*NN*” where *NN* is the member switch number.



Caution Do not use “@es” in the community strings you define for the switch. When the switch joins a cluster, any community string containing “@es” is deleted.

To add or change a SNMP Read community string:

Step 1 Enter up to 32 characters in the Read Community String field. The default for the first Read community string is public.

Step 2 Click **Add**.

To remove a SNMP Read community string:

Step 1 Select the community string from the Current list.

Step 2 Click **Remove**.

Assigning or Changing the SNMP Write Community Strings

The default for the first Write community string is private. You can assign up to four community strings to serve as passwords that enable the switch to validate SNMP read-write (Set) requests from a management station. The write managers you assign to the switch can use any of the switch Write community strings.

When the switch joins a cluster, the command switch assigns its first Write community string as the last Write community string for the member switch. If the joining Catalyst 1900 switch already has four Write community strings, the command switch overrides that fourth community string with its own first community string. When the switch leaves the cluster, the command-switch community string is deleted.

The command-switch string contains up to 27 characters and a suffix “@es*NN*” where *NN* is the member switch number.



Caution Do not use “@es” in the community strings you define for the switch. When the switch joins a cluster, any community string containing “@es” is deleted.

To add or change a SNMP Write community string:

Step 1 Enter up to 32 characters in the Write Community String field. The default for the first Write community string is private.

Step 2 Click **Add**.

To remove a SNMP Write community string:

Step 1 Select the community string from the Current list.

Step 2 Click **Remove**.

Assigning or Changing Trap Managers

A trap manager, or trap client, is an SNMP management station that receives traps, which are the system alerts generated by the switch. If no trap manager is defined, no traps are issued.

You can assign up to four trap managers and their accompanying community strings. A trap manager can use its accompanying community string only; it cannot use the community string of another trap manager.

Trap manager settings can be configured from the switch or, if the switch is a cluster member, from the command switch.

After you have assigned the trap manager(s), the switch generates, by default, the following traps:

- warmStart
- coldStart
- linkDown
- linkUp
- authenticationFailure
- newRoot
- topologyChange
- logonIntruder
- switchDiagnostic
- addressViolation
- broadcastStormControl
- rpsFailed
- ipAddressChange

For more information about traps, see the “Simple Network Management Protocol” section on page 1-24 and the “Accessing MIB Files” section on page 2-44.

Changing the SNMP Settings

To assign a trap manager and its community string:

Step 1 In the IP Address field, enter the IP address of the SNMP management station that can issue trap requests to the switch. Use dotted quad format (nnn.nnn.nnn.nnn).

If the switch is connected to a Domain Name System (DNS) server, you can enter the name of the trap manager instead.

Step 2 Enter a community string (up to 32 characters) in the Trap Manager Community String field.

Step 3 Click **Add**.

To remove a trap manager:

Step 1 Select the manager from the Current list.

Step 2 Click **Remove**.

Authentication Trap Generation

By default, authentication trap generation is enabled (**Enable Authentication Trap Generation** check box is selected). This option enables the switch to generate authentication traps, which alert a management station of SNMP requests not accompanied by a valid community string.

Note Even if this option is enabled, no traps are generated if no trap manager addresses or names are assigned. (See the “Assigning or Changing Trap Managers” section on page 3-39.)

To disable authentication trap generation:

Step 1 Deselect the **Enable** check box.

Step 2 Click **Apply**.

LinkUp/LinkDown Trap Generation

By default, linkUp/linkDown trap generation is enabled (**Enable LinkUp/LinkDown Trap Generation** check box is selected). This option enables the switch to generate linkDown traps when a port is suspended or disabled for any of these reasons:

- Secure address violation (address mismatch or duplication)
- Network connection error (loss of linkbeat or jabber error)
- Port disabled by management action

The switch generates linkUp traps when a port is enabled for any of these reasons:

- Presence of linkbeat
- Management intervention
- Recovery from an address violation or any other error

Note No more than one trap is sent every 5 seconds per port. The last trap generated in the 5-second interval is the one sent.

To disable linkUp/linkDown trap generation:

Step 1 Deselect the **Enable** check box.

Step 2 Click **Apply**.

Broadcast Storm Trap Generation

By default, broadcast storm trap generation is disabled (**Enable Broadcast Storm Trap Generation** check box is not selected). When this option is enabled, the switch generates SNMP alerts when the broadcast threshold is exceeded. The alert generated is the trapbroadcastStorm. A trap is generated every 30 seconds.

For information about broadcast storm control, see the “Broadcast Storm Control” section on page 3-76.

To enable broadcast storm trap generation:

Step 1 Select the **Enable** check box.

Step 2 Click **Apply**.

Changing the SNMP Settings

Address Violation Trap Generation

By default, address violation trap generation is enabled (**Enable Address Violation Trap Generation** check box is selected). This option enables the switch to generate SNMP alerts if an address violation occurs.

To disable address violation trap generation:

Step 1 Deselect the **Enable** check box.

Step 2 Click **Apply**.

Assigning or Changing Write Managers

A write manager is an SNMP management station that can issue write requests to the switch. You can assign up to four write managers. The switch allows write requests from only the specified write managers or from the command switch. The write managers you assign can use any of the switch Write community strings.



Caution If no write manager is assigned to the switch, any management station can modify the switch MIB objects.

Note The write manager option is not available from the command switch. To use this option, use the SNMP Management Page or the Network Management (SNMP) WRITE Configuration Menu.

To assign a write manager:

Step 1 Enter the IP address in the IP Address field. Use dotted quad format (nnn.nnn.nnn.nnn).

If the switch is connected to a DNS server, you can enter the name of the write manager instead.

Step 2 Click **Add**.

To remove a write manager:

Step 1 Select the manager from the Current list.

Step 2 Click **Remove**.

Changing the Spanning-Tree Protocol Settings

The Spanning-Tree Protocol (STP) constructs network topologies that do not contain loops. When the network configuration changes, STP transparently reconfigures bridges and switches to avoid the creation of loops. STP avoids loops by placing ports in a forwarding or blocking state and establishes redundant paths (in the event of lost connections).

The following are two examples for using STP:

- **Redundant connectivity**—You can create a redundant backbone with STP by connecting two of the ports on a switch 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, STP uses the high-speed link. If the speed of the two links is the same, the port priority and port ID are added together, and the link with the lowest value is disabled.
- **Accelerated address aging**—Dynamic addresses are aged and dropped from the address table after a configurable period of time. The default for aging dynamic addresses is 5 minutes. However, a reconfiguration of the spanning tree can cause many station locations to change. Because this could mean that many stations are unreachable for 5 minutes or more, the address-aging time is accelerated so that station addresses can be dropped from the address table and then relearned. The accelerated-aging value is the same as the forward-delay parameter value when STP reconfigures.

Changing the Spanning-Tree Protocol Settings

A separate spanning-tree instance runs on each bridge group, and each bridge group participates in a separate spanning tree. Each switch in a spanning tree adopts the Hello, Max age, and Delay parameters of the root bridge regardless of how it is configured. Overlapping ports (ports that belong to more than one bridge group) participate in all spanning trees to which they belong. All ports on the switch support STP, and STP is managed through the standard Bridge MIB.

Note From the switch manager, you can only configure the STP settings for bridge group 1 (the management bridge group) or VLAN 1 (the management VLAN).

Overlapping ports should be connected to end nodes only, not to other bridges. To configure the STP settings for other bridge groups on the switch, use the Spanning Tree Configuration Menu on the management console.

For more information about bridge groups and to configure bridge groups, see the Bridge Group Configuration Menu and the “Spanning Tree Configuration Menu” on page 31. For information about VLANs, refer to the *Catalyst 1900 Series and Catalyst 2820 Series Enterprise Edition Software Configuration Guide*.

To display the Spanning-Tree Management Page (Figure 3-8), click **STP** on the menu bar.

Figure 3-8 Spanning-Tree Management Page

[HOME](#)
[PORT](#)
[ADDRESS](#)
[SNMP](#)
[STP](#)
[CDP](#)
[SPAN](#)
[CONSOLE](#)
[STATISTICS](#)
[SYSTEM](#)
[CGMP](#)

Member Switch Host Name: s202-1 **Command Switch IP:** 10.1.126.35

Spanning-Tree Management

Enable Spanning Tree: ☒ ←

Spanning Tree Operating Parameters

Bridge ID:	7FFF.0010.F627.C300	Designated Root:	2000.0090.0C71.A400
Number of Member Ports:	27	Root Port:	3
Max Age:	20 seconds	Root Path Cost:	3167
Hello Time:	2 seconds	Forward Delay:	15 seconds
Topology Changes:	55	Last TopChange:	0db0h04m04s

Spanning Tree Configurations

Bridge Priority:	<input type="text" value="32767"/>	Max Age:	<input type="text" value="20"/> seconds
	[0-65535 [32768]]		[6-40 [20]]
Hello Time:	<input type="text" value="2"/> seconds	Forward Delay:	<input type="text" value="15"/> seconds
	[1-10 [2]]		[4-30 [15]]

Port Parameters

Module	Port	State	Forward Transitions	Path Cost [1-65536 [100]]	Priority [0-255]	Port Fast Mode
	Ethernet 0/1	Forwarding	1	<input type="text" value="100"/>	<input type="text" value="128"/>	<input checked="" type="checkbox"/> Enable
	Ethernet 0/2	Forwarding	1	<input type="text" value="100"/>	<input type="text" value="128"/>	<input checked="" type="checkbox"/> Enable
	Ethernet 0/3	Forwarding	1	<input type="text" value="100"/>	<input type="text" value="128"/>	<input checked="" type="checkbox"/> Enable
	Ethernet 0/4	Forwarding	1	<input type="text" value="100"/>	<input type="text" value="128"/>	<input checked="" type="checkbox"/> Enable

Set the switch to use or not use the Spanning-Tree Protocol.

Displays the read-only STP settings for the current root switch. The Bridge ID field identifies the root switch.

Set the values that take effect when the switch becomes the root switch.

Lists the port-specific parameters that affect how each port responds if a loop is formed.

Enabling or Disabling Spanning-Tree Protocol

By default, STP is enabled (**Enable Spanning Tree** check box is selected). To disable STP:

Step 1 Deselect the **Enable Spanning Tree** check box.

Step 2 Click **Apply**.

Spanning-Tree Root Settings

The Operating Parameters section displays the following read-only STP settings for the current root switch, which could be defined on another switch.

Bridge ID	Unique hexadecimal ID number that has a bridge priority and a unique MAC address.
Number of Member Ports	Number of ports configured with STP.
Max Age	Number of seconds a bridge waits for STP configuration messages before attempting a reconfiguration.
Hello Time	Number of seconds between the transmission of STP configuration messages. All bridges send configuration messages during reconfiguration to elect the designated root bridge. After STP completes its network discovery, only designated bridges send configuration messages.
Topology Changes	Number of bridge topology changes experienced by the network. A topology change occurs as ports on any bridge change from a nonforwarding to a forwarding state or when a new root is selected.
Designated Root	ID number of the bridge identified as the root by the STP.
Root Port	Port on this bridge with the lowest-cost path to the root bridge. This option identifies the port through which the path to the root bridge is established. N/A is displayed when STP is disabled or when this bridge is the root bridge.
Root Path Cost	Cost of the path from this bridge to the root bridge shown in the Designated Root field. It equals the path cost parameters held for the root port.
Forward Delay	Number of seconds before a port changes from its STP learning and listening states to a forwarding state. Every bridge on the network ensures that no loop is formed before the port can forward packets.
Last TopChange	Number of days (d), hours (h), minutes (min), and seconds (s) since the last topology change.

Changing the Spanning-Tree Options for the Switch

The Spanning Tree Configuration section displays a list of STP parameters that this switch will use when it is the root switch.

Note Modifying the spanning-tree settings causes a temporary loss of connectivity while the network reconfigures. STP requires approximately 30 seconds to complete its discovery of the network, and the switch does not forward packets during this time.

Note For information about VLANs and the Uplink Fast option, refer to the *Catalyst 1900 Series and Catalyst 2820 Series Enterprise Edition Software Configuration Guide*.

To change the STP configuration on this switch:

Step 1 Enable STP if you have previously disabled it:

- (a) Select the **Enable Spanning Tree** check box.
- (b) Click **Apply**.

Note You can slightly improve switch performance by disabling STP. However, disable STP only if you are sure there are no loops in your network topology. With STP disabled and loops present in the topology, network performance is degraded by excessive traffic and indefinite packet duplication.

Step 2 In the Bridge Priority field, enter the value (0 to 65535) used in determining the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. The default is 32768.

Changing the Spanning-Tree Protocol Settings

- Step 3** In the Hello Time field, enter the number of seconds (1 to 10) between the transmission of STP configuration messages. The default is 2.
- Step 4** In the Max Age field, enter the number of seconds (6 to 40) a switch waits for STP configuration messages before it attempts a reconfiguration. After this period expires, other bridges recognize that the root has not sent a configuration message, and a new root is selected. The default is 20.
- Step 5** In the Forward Delay field, enter the number of seconds (4 to 30) a port waits before changing from its STP learning and listening states to the forwarding state. This delay time is necessary to ensure that no loop is formed before the switch forwards a packet. The default is 15.

Note Spanning-Tree Protocol also uses this value to accelerate address aging when the spanning tree is reconfigured.

- Step 6** Click **Apply**.

Changing Spanning-Tree Settings for Bridge Group 1 and Its Ports

Note Modifying the spanning-tree settings causes a temporary loss of connectivity while the network reconfigures. STP requires approximately 30 seconds to complete its discovery of the network, and the switch does not forward packets during this time.

To change the spanning-tree parameters for a port, follow these steps:

Step 1 Enable STP if you have previously disabled it:

- (a) Select the **Enable Spanning Tree** check box.
- (b) Click **Apply**.

Note You can slightly improve switch performance by disabling STP. However, disable STP only if you are sure there are no loops in your network topology. With STP disabled and loops present in the topology, network performance is degraded by excessive traffic and indefinite packet duplication.

Step 2 In the Path Cost column, enter a number from 1 to 65535 for each port. The default for the 10-Mbps ports is 100. The default for the 100-Mbps ports is 10.

The path cost is inversely proportional to the LAN speed of the network interface at the port. A high path cost means the port has low bandwidth and should not be used, if possible. A lower path cost represents higher-speed transmission; this setting can affect which port remains enabled in the event of a loop.

This option also affects which port is to remain enabled by STP if another bridge device forms a loop with the switch.

Note We recommend setting the path cost to 100 on the 10-Mbps ports.

Changing the Spanning-Tree Protocol Settings

Step 3 In the Priority column, enter a number from 0 to 255 for each port. The default is 128. The lower the number, the higher the priority. The higher priority port remains enabled by STP if two ports form a loop.

Step 4 In the Port Fast Mode column, select a port, and select the check box to enable the Port Fast mode. The default for the 10-Mbps ports is enabled (**Port Fast Mode** check box is selected). The default for the 100-Mbps ports is disabled (**Port Fast Mode** check box is not selected).

Port Fast mode immediately brings a port from the blocking state into the forwarding state by eliminating the forward delay (the amount of time a port waits before changing from its STP learning and listening states to the forwarding state).

Note Port Fast Mode-enabled ports should only be used for end-station attachments.

When the switch is powered up, the forwarding state, even if Port Fast mode is enabled, is delayed to allow the Spanning-Tree Protocol to discover the topology of the network and ensure no temporary loops are formed. Spanning-tree discovery takes approximately 30 seconds to complete, and no packet forwarding takes place during this time. After the initial discovery, Port Fast-enabled ports transition directly from the blocking state to the forwarding state.

Step 5 Click **Apply**.

Port and Forwarding STP States

The State column displays the state of the port. A port can be in one of the following states:

- | | |
|------------|---|
| Blocking | The port is not forwarding frames and is not learning new addresses. |
| Listening | The port is not forwarding frames but is progressing toward a forwarding state. The port is not learning addresses. |
| Learning | The port is not forwarding frames but is learning addresses. |
| Forwarding | The port is forwarding frames and learning addresses. |

Disabled The port has been removed from STP operation. You need to re-enable the port.

The Forward Transitions column displays the number of times STP changed forwarding states.

Changing the CDP Settings

The Cisco Discovery Protocol (CDP) enables the switch to advertise its existence to other Cisco devices on the network. When CDP is enabled, the switch and the network management applications have an accurate picture of the network at any time because CDP gathers information about device types, links between devices, and the number of interfaces on each device.

Before the switch joins a cluster, CDP version 2 must be enabled on the switch. For information about enabling this option, see the “CDP Configuration/Status Menu” section on page 4-36. For information about cluster management and membership, refer to the *Cisco IOS Desktop Switch Software Configuration Guide, Catalyst 2900 Series XL and Catalyst 3500 Series XL Cisco IOS Release 12.0(5)XP*.

To display the CDP Management Page (Figure 3-9), click **CDP** on the menu bar.

Changing the CDP Settings

Figure 3-9 CDP Management Page

The screenshot shows the CDP Management page with a navigation bar at the top containing links: HOME, PORT, ADDRESS, SNMP, STP, CDP, SPAN, CONSOLE, STATISTICS, SYSTEM, and CGMP. Below the navigation bar, it displays 'Member Switch Host Name: s202-1' and 'Command Switch IP: 10.1.126.35'. The main section is titled 'CDP Management' and contains a 'Discovered Neighboring Devices' section. This section has a list box showing '10.1.126.35' and three buttons: 'Browse', 'Telnet', and 'Details...'. Annotations point to these buttons: 'Browse' is described as 'Accesses the web console of a connected neighboring device.', 'Telnet' as 'Opens a Telnet session and logs you into a connected neighboring device.', and 'Details...' as 'Displays detailed information about a connected neighboring device.' Below this is the 'CDP Options' section. It includes 'Packet Hold Time' set to '180 seconds [5-255 [180]]' and 'Packets Transmission Time' set to '60 seconds [5-900 [60]]'. Annotations explain these: 'Packet Hold Time' is 'Length of time a neighboring device retains CDP information it received from this switch. The packet hold time should be higher than the packet transmission time.' and 'Packets Transmission Time' is 'Length of time between transmissions of CDP messages. The packet transmission time should be lower than the packet hold time.' The 'Select the Ports to be CDP Enabled:' section shows two list boxes: 'CDP Enabled' (containing Ethernet 0/2 through 0/8) and 'CDP Disabled' (empty). Between them are '<< Enable <<' and '>> Disable >>' buttons. A bracket under these elements is annotated: 'Select the ports to participate in exchanging CDP information with other Cisco devices.'

HOME PORT ADDRESS SNMP STP CDP SPAN CONSOLE STATISTICS SYSTEM CGMP

Member Switch Host Name: s202-1 Command Switch IP: 10.1.126.35

CDP Management

Discovered Neighboring Devices

10.1.126.35

Browse

Telnet

Details...

Accesses the web console of a connected neighboring device.

Opens a Telnet session and logs you into a connected neighboring device.

Displays detailed information about a connected neighboring device.

CDP Options

Packet Hold Time: 180 seconds [5-255 [180]]

Packets Transmission Time: 60 seconds [5-900 [60]]

Length of time a neighboring device retains CDP information it received from this switch. The packet hold time should be higher than the packet transmission time.

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

Select the Ports to be CDP Enabled:

CDP Enabled:

Ethernet 0/2

Ethernet 0/3

Ethernet 0/5

Ethernet 0/6

Ethernet 0/7

Ethernet 0/8

<< Enable <<

>> Disable >>

CDP Disabled:

Select the ports to participate in exchanging CDP information with other Cisco devices.

26584

Displaying CDP Neighbors

The Discovered Neighboring Devices list shows the devices with which the switch exchanges CDP messages. To display information about neighboring devices:

- Step 1** Select a device from the Discovered Neighboring Devices list.
- Step 2** Click one of these buttons:
- Click **Browse** to access the web console of a neighboring device. The neighbor must be a device that has web-console support.
 - Click **Telnet** to open a Telnet session and log into a neighboring device.
 - Click **Details** to display the detailed CDP information currently stored in the switch.

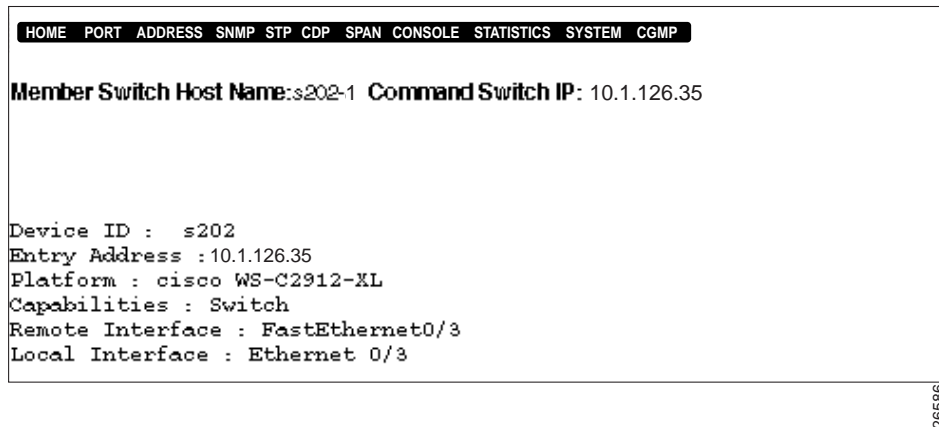
When you select a neighboring device and click **Details** on the CDP Management page, the switch manager displays the following information about that device (see CDP Details Page, Figure 3-10):

Device ID	Neighbor host name.
Entry address	IP address.
Platform	Description of the product platform to which the neighbor belongs.
Capabilities	Description of the type of device (such as, repeater or switch).
Remote Port	Description of the port on the neighbor to which this switch is connected.
Local Port	Number and description of the port on this switch to which the neighbor is connected.

If a neighboring Catalyst 1900 or Catalyst 2820 cluster member does not have an IP address before it joins a cluster, the command switch IP address is displayed in the Entry Address field when you select that Catalyst 1900 or Catalyst 2820 cluster member, and click **Details**.

Changing the CDP Settings

Figure 3-10 CDP Details Page



The screenshot shows a web interface for CDP details. At the top is a navigation bar with links: HOME, PORT, ADDRESS, SNMP, STP, CDP, SPAN, CONSOLE, STATISTICS, SYSTEM, and CGMP. Below the navigation bar, the text reads: "Member Switch Host Name: s202-1 Command Switch IP: 10.1.126.35". Further down, the following details are listed: "Device ID : s202", "Entry Address : 10.1.126.35", "Platform : cisco WS-C2912-XL", "Capabilities : Switch", "Remote Interface : FastEthernet0/3", and "Local Interface : Ethernet 0/3". A vertical page number "26586" is visible on the right side of the screenshot.

Changing the CDP Settings

To change the global CDP settings for the switch:

- Step 1** In the Packet Hold Time field, enter the number of seconds (between 5 and 255) that a neighboring device keeps the CDP neighbor information received from this switch. The default is 180 seconds.

If a neighboring device does not receive a CDP message before the hold time expires, the device drops this switch as a neighbor. The packet hold time should be higher than the packet transmission time.

- Step 2** In the Packet Transmission Time field, enter the number of seconds (between 5 and 900) between transmissions of CDP messages. The default is 60 seconds. The packet transmission time should be lower than the packet hold time.

- Step 3** Click **Apply**.

Enabling or Disabling CDP on a Port

By default, CDP is enabled on all ports on the switch. If you do not want a port to exchange information with Cisco devices, you can disable CDP on that port. To disable CDP on a port:

Step 1 Select the port from the CDP Enabled list.

Step 2 Click **Disable**.

Note Only 15 ports can be selected at a time. Repeat these steps until you have removed the ports that you no longer want to participate in CDP exchanges.

To enable CDP on a port:

Step 1 Select the port from the CDP Disabled list.

Step 2 Click **Enable**.

Note Only 15 ports can be selected at a time. Repeat these steps until you have added the ports that you want to participate in CDP exchanges.

Port Monitoring (Switched Port Analyzer)

The remote monitoring (RMON) capability on the switch helps you monitor network traffic traversing the switch, and with the Switched Port Analyzer (SPAN) feature, you can use a single network analyzer to monitor traffic on any of the switch ports. You simply attach the network analyzer to a switch port, using that port as a monitoring port. You can also use a network analyzer on the monitoring port to troubleshoot network problems by examining the traffic on other Cisco switched ports or segments.

By default, no port on the switch is designated as the monitoring port, and no ports on the switch are monitored. Remember the following restrictions when monitoring ports:

- The monitoring port cannot be a member of more than one bridge group.
- Do not make bridge group membership changes on the monitoring port or monitored ports until after you disable monitoring.

Note STP and BOOTP are disabled on the enabled monitor port. The flooding of unregistered multicast packets and unknown unicast packets is also disabled.

Note Enable monitoring only for problem diagnosis. Disable monitoring during normal operation so that switch performance is not degraded.

To display the SPAN Configuration Page (Figure 3-11), click **SPAN** on the menu bar.

Figure 3-11 SPAN Configuration Page

HOME

PORT

ADDRESS

SNMP

STP

CDP

SPAN

CONSOLE

STATISTICS

SYSTEM

CGMP

Member Switch Host Name: s202-1 Command Switch IP: 10.1.126.35

SPAN Configuration

Port Monitoring

Capturing Frames to the Monitoring Port:

Select Monitoring Port:

☐ ← Set the switch to monitor or not monitor traffic on the selected monitored ports.

none ↓ Select the monitoring port (the port to which captured frames are sent).

Select the Ports to be Monitored:

Ports Monitored:

<< Add <<

>> Remove >>

Ports Not Monitored:

Ethernet 0/1
Ethernet 0/2
Ethernet 0/3
Ethernet 0/4
Ethernet 0/5
Ethernet 0/6

Select the ports to be monitored.

26588

Port Monitoring (Switched Port Analyzer)

By default, port monitoring is disabled (**Capturing Frames to the Monitoring Port** check box is not selected).

To enable port monitoring on the switch and its port(s):

- Step 1** Select the **Capturing Frames to the Monitoring Port** check box.
- Step 2** Select the monitoring port (the port to which captured frames are sent) from the Select Monitoring Port drop-down list.
- You can designate any port as the monitoring port, but the following restrictions apply:
- The monitoring port cannot be a member of more than one bridge group.
 - Do not make bridge group membership changes on the monitoring port or monitored ports until after you disable monitoring.
- Step 3** Select the port(s) you want to monitor from the Port Not Monitored list.
- Step 4** Click **Add**.

Note Only 15 ports can be selected at a time. Repeat these steps until you have added all of the ports that you want to monitor.

To disable port monitoring on a port or ports:

- Step 1** Select the port(s) that you no longer want to monitor from the Ports Monitored list.
- Step 2** Click **Remove**.

Note Only 15 ports can be selected at a time. Repeat these steps until you have removed all of the ports that you no longer want to monitor.

Changing the Console Port Settings and Upgrading the Firmware

Cisco periodically provides new firmware to implement enhancements and maintenance releases. New firmware releases can be downloaded from Cisco Connection Online (CCO), the Cisco Systems' customer web site available at the following URLs: www.cisco.com, www-china.cisco.com, and www-europe.cisco.com.

The Firmware Version field displays the firmware version being used by the switch.



Caution If you interrupt the transfer by turning the switch off and on, the firmware could get corrupted. For recovery procedures, see the “Recovering from Corrupted Firmware” section on page 5-13.

Note When you download the firmware to Flash memory, the switch does not respond to commands for approximately 1 minute. This is normal and correct. Unlike the management console, the switch manager does not provide any status on the download. Do not turn off the switch until after the switch resets and begins using the new firmware.

To display the Console and Upgrade Configuration Page (Figure 3-12), click **Console** on the menu bar.

Changing the Console Port Settings and Upgrading the Firmware

Figure 3-12 Console and Upgrade Configuration Page

HOME PORT ADDRESS SNMP STP CDP SPAN CONSOLE STATISTICS SYSTEM CGMP

Member Switch Host Name: s202-1 Command Switch IP: 10.1.126.35

Console and Upgrade Configuration

Console

Baud Rate: 9600 baud

Data Bits: 8 bits

Stop Bits: 1 bit(s)

Parity Setting: None

Management Console Inactivity Timeout: 0 seconds [30-65500 [0]]

Initialization String for Modem:

Enable Auto Baud (Match Remote Baud Rate): ☒

Enable Auto Answer: ☒

Firmware Upgrade Options

Firmware Version: V9.00.00 written from 10.1.126.35

Server IP Address or Name of TFTP Server:

Filename for Firmware Upgrades:

Accept Upgrade Transfer from Other Hosts: ☐

System TFTP Upgrade

Before using the XMODEM protocol to download the upgrade file to the switch, make sure the settings of the switch console port and the management station match.

Length of time before the management console times out because of inactivity.

Displays the firmware version used by the switch.

Available when the switch has its own IP address.

26590

Configuring the Switch Console Port

The console port on the switch provides terminal and PC access to the switch. After the switch is installed, be sure to configure the console port settings of the switch to match the settings of the terminal or PC.

These are the default settings of the switch console port:

- Baud rate default is 9600.
- Data bits default is 8.

Note If the data bits option is set to 8, set the parity option to None.

- Stop bits default is 1.
- Parity settings default is None.

If you change any of these settings, click **Apply** to save your changes.

Management Console Inactivity Timeout

By default, the management console inactivity timeout is 0 (which means the console session does not time out). You can change the number of seconds that the management console can wait without activity before it times out. After timeout, you must reenter the password.

To change the inactivity timeout setting:

Step 1 Enter the number of seconds (0, or 30 to 65500) in the Management Console Inactivity Timeout field.

Step 2 Click **Apply**.

Changing the Console Port Settings and Upgrading the Firmware

Modem Initialization String

The switch uses the initialization string to initialize the modem connected to the console port. This string must match your modem requirement.

Note Do not use an AT prefix or end-of-line suffix.

Auto Baud

By default, auto baud (match remote baud rate) is enabled (**Enable Auto Baud** check box is selected). This option enables the switch to automatically match the same or lower baud rate of an incoming call. After the call, the switch reverts to its configured rate.

Auto Answer

By default, auto answer is enabled (**Enable Auto Answer** check box is selected). This option enables the switch to automatically answer calls.

Upgrading the Switch Firmware

The Firmware Version field displays the firmware version being used by the switch.

The following sections provide instructions on how to upgrade the switch firmware:

- “Downloading Switch Firmware from a TFTP Server” section on page 3-63
- “Downloading Switch Firmware from a TFTP Client” section on page 3-64

Downloading Switch Firmware from a TFTP Server



Caution If you interrupt the transfer by turning the switch off and on, the firmware could get corrupted. For recovery procedures, see the “Recovering from Corrupted Firmware” section on page 5-13.

Follow these steps to download the latest firmware from a TFTP server to your switch.

- Step 1** Download the upgrade file from CCO into an appropriate directory on your TFTP server.
- Step 2** Enter the IP address in the Server: IP Address or Name of TFTP Server field. Use dotted quad format (nnn.nnn.nnn.nnn).

If the switch is connected to a Domain Name System (DNS) server, you can enter the name of the TFTP server instead.
- Step 3** Enter the upgrade filename (up to 80 characters) in the Filename for Firmware Upgrades field.
- Step 4** Click **System TFTP Upgrade** to download the upgrade file from the TFTP server to the switch.
- Step 5** Click **OK** on the confirmation prompt.

Note When you download the firmware to Flash memory, the switch does not respond to commands for approximately 1 minute. This is normal and correct. Unlike the management console, the switch manager does not provide any status on the download. Do not turn off the switch until after the switch resets and begins using the new firmware.

After the existing firmware validates the file, the new image is transferred into Flash memory, the switch resets, and the new firmware begins executing. If the upgrade file is invalid, the temporary image is discarded, the existing firmware continues to execute, and the firmware upgrade ends.

- Step 6** Click the browser **Reload** button to refresh the Console and Upgrade Configuration Page.
- Step 7** Ensure that the Firmware Version field displays the updated firmware version.

Downloading Switch Firmware from a TFTP Client



Caution If you interrupt the transfer by turning the switch off and on, the firmware could get corrupted. For recovery procedures, see the “Recovering from Corrupted Firmware” section on page 5-13.

Follow these steps to download the latest firmware from a TFTP client to your switch.

- Step 1** Download the upgrade file from CCO into an appropriate directory on your TFTP client.
- Step 2** From the client management station, establish a TFTP session with the IP address of the switch. Make sure the client station is in binary transfer mode.
- Step 3** Select the **Accept Upgrade Transfer from Other Hosts** check box. By default, this check box is not selected.

Note To prevent unauthorized upgrades, deselect this check box after you upgrade the firmware.

- Step 4** Download the upgrade file from the client station to the switch, using the TFTP user interface or the appropriate command for the put operation (such as, **put upgrade_filename**).

Note When you download the firmware to Flash memory, the switch does not respond to commands for approximately 1 minute. This is normal and correct. Unlike the management console, the switch manager does not provide any status on the download. Do not turn off the switch until after the switch resets and begins using the new firmware.

After the existing firmware validates the file, the new image is transferred into Flash memory, the switch resets, and the new firmware begins executing. If the upgrade file is invalid, the temporary image is discarded, the existing firmware continues to execute, and the firmware upgrade ends.

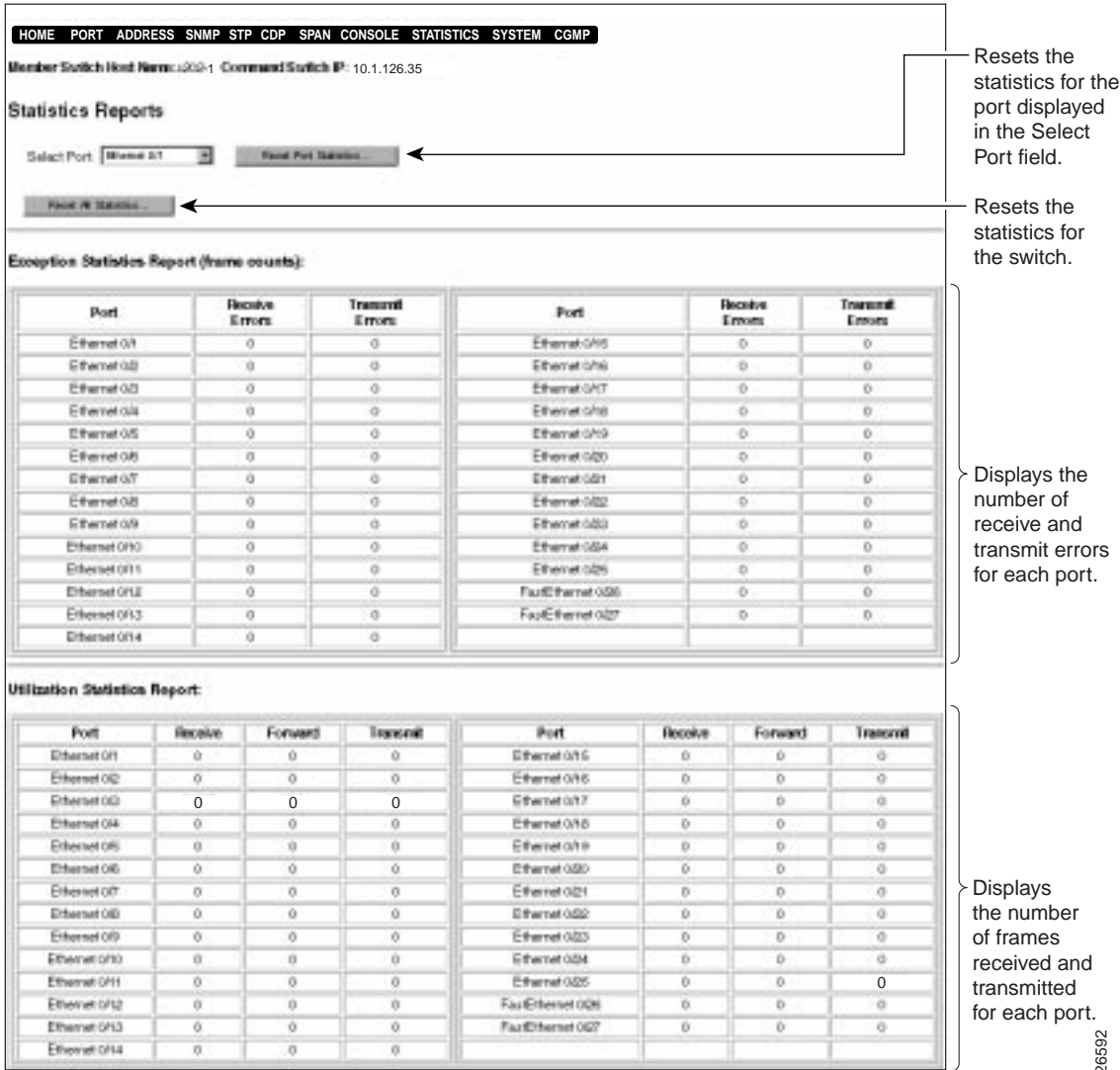
- Step 5** Click the browser **Reload** button to refresh the Console and Upgrade Configuration Page.
- Step 6** Ensure that the Firmware Version field displays the updated firmware version.
- Step 7** Deselect the **Accept Upgrade Transfer from Other Hosts** check box.

Exception and Utilization Statistics

The Statistics Reports Page (Figure 3-13) displays the exception and utilization statistics for the switch. To display this page, click **Statistics** on the menu bar.

Exception and Utilization Statistics

Figure 3-13 Statistics Reports Page



26592

Resetting Port and Switch Statistics

To reset the statistics for a switch port:

Step 1 Select the port from the Select Port list.

Step 2 Click **Reset Port Statistics**.

To reset the statistics for all ports on the switch, click **Reset All Statistics**.

The switch manager does not automatically refresh the statistics shown on this page. Click the browser **Reload** button to refresh the statistics shown on this page.

Exception Statistics

This report displays the number of receive and transmit errors for each port.

Receive	Number of giants and FCS and alignment errors
Transmit	Number of excessive deferrals, late collisions, jabber errors, and other transmit errors

Utilization Statistics

This report displays the number of bytes received and transmitted for each port.

Receive	Number of bytes received in good packets
Forward	Number of good frames forwarded
Transmit	Number of bytes transmitted

Changing the System Management Settings

The system management settings include the switch IP information and the settings for switch performance and flood and traffic control. To display the System Management Page (Figure 3-14), click **System** on the menu bar.

Figure 3-14 System Management Page

HOME
PORT
ADDRESS
SNMP
STP
CDP
SPAN
CONSOLE
STATISTICS
SYSTEM
CGMP

Member Switch Host Name:s202-1
Command Switch IP: 10.1.126.35

System Management

IP Address:
Subnet Mask:
Domain Name:
Default Gateway:
IP Address of DNS Server 1:
IP Address of DNS Server 2:
Use Routing Information Protocol:
Switching Mode:
Enable the Use of Store-and-Forward for Multicast:
Action Upon Address Violation:
Network Port:
Half-Duplex Back Pressure for All 10-Mbps Ports:
Enhanced Congestion Control for All 10-Mbps Ports:

☒
Fragment Free
☐
Suspend
none
Disabled
Disabled

Switch-specific IP information is required to manage the switch as an individual switch. As a cluster member, the switch is managed through the IP address of the command switch.

Set the parameters that can improve switch performance and flooding and traffic control.

Broadcast Storm Control

Action Upon Exceeding Broadcast Threshold:
Broadcast Threshold:
Broadcast Reenable Threshold:

Ignore
500
250

packets/second [10-14400 [500]]
packets [10-14400 [250]]

Set parameter to control the forwarding of broadcast packets.

26594

Assigning or Changing IP Information

Typically, after the switch is installed, an IP address is assigned to the switch. (See the “Assigning IP Information and a Password to the Switch” section on page 2-19.)

IP information identifies the switch on the network and is required to configure and monitor it as an individual switch. When you assign the switch its own IP address, you can manage it from its management interfaces (switch manager, management console, SNMP, or CLI). The switch retains its own IP address even when it joins or leaves a switch cluster.

If you do not assign an IP address to the switch, you must add the switch to a switch cluster and manage it through the command switch. Whether or not the switch has its own IP address, when the switch is a cluster member, it is managed and communicates with other member switches through the IP address of the command switch. If the switch leaves the cluster and it does not have its own IP address, you then must assign IP information to it to manage and monitor it as a nonmember switch.

Note We recommend that you assign an IP address to the switch even if the switch is or will be a cluster member so that if the switch is removed from the cluster, it remains manageable as a nonmember switch.

Note You access the switch manager from a management station that is connected to one of the switch ports. Therefore, make sure that you do not disable or otherwise misconfigure the port through which you are communicating with the switch. You might want to write down the port number to which you are connected. Make changes to the switch IP information with care.

For information about IP information in switch clusters, refer to the *Cisco IOS Desktop Switch Software Configuration Guide, Catalyst 2900 Series XL and Catalyst 3500 Series XL Cisco IOS Release 12.0(5)XP*.

To change the switch IP information:

Step 1 Enter a new IP address for the switch in the IP Address field. Use dotted quad format (nnn.nnn.nnn.nnn).

If the switch is connected to a network that has a Dynamic Host Configuration Protocol (DHCP)/Bootstrap Protocol (BOOTP) server, the server automatically assigns it an IP address.

This field displays the IP address assigned to the switch. If the switch does not have an IP address, this field displays 0.0.0.0.



Caution Changing the switch IP address on this page will end your switch manager session. You will need to open a new session and enter the new IP address in the URL field if you are using Communicator (the Address field if you are using Internet Explorer).

Note We recommend that you assign an IP address to the switch even if the switch is or will be a cluster member so that if the switch is removed from the cluster, it remains manageable as a nonmember switch.

Step 2 Enter the subnet mask for the switch in the Subnet Mask field.

Subnet masks exist only if the network has been divided up into subnetworks.

Step 3 In the Domain Name field, enter the domain name (up to 62 characters) of the Domain Name System (DNS) server to which the switch is associated (such as cisco.com).

Step 4 In the Default Gateway field, enter the IP address of the default gateway. Use dotted quad format (nnn.nnn.nnn.nnn).

The default gateway is the router that the switch uses to reach IP subnets other than the local subnet to which the switch is attached. A default gateway is also necessary if the management station from which the switch is to be managed is not on the same IP subnet as the switch.

For automatic IP gateway assignment, see the “Routing Information Protocol” section on page 3-72.

Changing the System Management Settings

- Step 5** In the IP Address of DNS Server 1 and 2 fields, enter the IP address(es) of the DNS server(s). For more information about the DNS server, see the “Domain Name System Servers” section on page 3-72.
- Step 6** Click **Apply**.

Domain Name System Servers

A network device can be identified through its IP address or its associated host name. Domain Name System (DNS) servers maintain name-to-address mappings.

If you enter the device name when using the switch management interfaces, the DNS server associated with the switch looks up the device IP address. The switch can be associated to up to two DNS servers.

To associate a DNS server to the switch:

- Step 1** Enter the IP address of the DNS server in the IP Address of DNS Server field. Use dotted quad format (nnn.nnn.nnn.nnn).
- Step 2** Click **Apply**.

Routing Information Protocol

By default, the Routing Information Protocol (RIP) is enabled (**Use Routing Information Protocol** check box is selected). RIP automatically discovers and assigns an IP gateway to the switch.

The default gateway is the router that the switch uses to reach IP subnets other than the local subnet to which the switch is attached. A default gateway is also necessary if the management station from which the switch is to be managed is not on the same IP subnet as the switch.

Switch Performance and Flooding and Traffic Control

Switching Modes

By default, the switching mode is FragmentFree (cut-through). The switching mode determines how quickly the switch forwards a packet and, therefore, how much latency the packet experiences. *Latency* is the delay between the time a port begins to receive a packet and the time the port begins to transmit the packet to a destination port. FragmentFree mode filters out collision fragments before forwarding. Store-and-forward stores complete packets and checks for errors before forwarding.

The switch uses these switching modes:

- FragmentFree—This mode is *cut-through* switching. The FragmentFree mode filters out collision fragments (the majority of packet errors) before forwarding begins. In a properly functioning network, collision fragments are packets with less than 64 bytes. In FragmentFree mode, the switch waits until 64 bytes are received (determines the received packet is not a collision fragment) before forwarding the packet. In FragmentFree mode, latency is measured as first-bit-received to first-bit-transmitted or “First-In, First-Out” (FIFO).

If latency is an issue, use FragmentFree switching.

- Store-and-forward—This mode stores complete packets and checks for errors before transmission. In this mode, latency is measured as last-bit-received to first-bit-transmitted or “Last-In, First-Out” (LIFO). This latency does not include the time to receive the entire packet, which can vary according to packet size. At 10 Mbps, the packet receipt time varies between 51.2 microseconds and 1.2 milliseconds. At 100 Mbps, the packet receipt time varies between 5.12 and 122 microseconds. The store-and-forward mode is always used for broadcast packets and transfers from 10-Mbps to 100-Mbps ports.

Store-and-forward is the most error-free form of switching, but the forwarding latency is higher than FragmentFree (cut-through) switching. If you have frame check sequence (FCS) or alignment errors, use the store-and-forward mode so that packets with errors are filtered and not propagated to the rest of the network.

Changing the System Management Settings

Although Table 3-11 shows store-and-forward experiencing the lowest latency, the figures do not include the time it takes to receive the packet, which varies according to the packet size. Table 3-12 shows the minimum and maximum packet reception latencies, which you need to add to the store-and-forward latencies in Table 3-11.

Table 3-11 **FIFO Switching Latencies**

Switching Mode	10 Mbps to 10 Mbps	10 Mbps to 100 Mbps	100 Mbps to 100 Mbps	100 Mbps to 10 Mbps
FragmentFree (cut-through)	70 microsec	–	9 microsec	10 microsec
Store-and-forward	7 microsec + PRL	7 microsec + PRL	3 microsec + PRL	3 microsec + PRL

Table 3-12 **Packet Reception Latencies (PRL)**

Link Speed	Minimum Latency	Maximum Latency
10 Mbps	51.2 microsec	1224 microsec
100 Mbps	5.1 microsec	122.4 microsec

Store-and-Forward for Multicast Frames

By default, store-and-forward for multicast frames is disabled (**Enable the Use of Store-and-Forward for Multicast** check box is not selected). If this option is disabled, the switch forwards multicast frames according to the switching mode. The store-and-forward mode is always used for broadcast frames.

Action Upon Address Violations

The default action is Suspend. An address violation occurs if a secure port receives a source address statically assigned to another port or if a secure port tries to learn more than a defined number of addresses. From the Action Upon Address Violation drop-down list, you can select the action a port takes if an address violation occurs:

- Suspend—The port stops forwarding until a packet with a valid source address is received.
- Disable—The port is permanently disabled, and you will have to re-enable it.
- Ignore—The port status remains unchanged.

For information about secure ports, see the “Securing a Port” section on page 3-33.

Network Port

A unicast address identifies one unique device on the network. However, if the switch has not received packets from the device for a while (longer than the aging period), the switch removes the device address from its address table, and the address is then an unknown unicast address. The switch must flood (send to all ports except the one the packet is received on) packets destined for the unknown unicast address in order to ensure the device receives the packet. Once the switch learns the location of the device, this flooding stops.

The use of a network port can eliminate this type of flooding. The network port that you select from the Network Port drop-down list is the destination port for all packets with unknown unicast addresses. By default, no port is assigned as the network port.

The network port

- Does not learn addresses.
- Serves only within the bridge groups of which the Network Port is member.
- Is usually connected to a legacy network or backbone.
- Cannot be a secure port.
- Cannot be port A or B if the following enterprise edition software features are enabled: Fast EtherChannel mode or VLAN or ISL trunking.

For more information about unicast addresses, see the “Enabling or Disabling Flooding of Unknown MAC Addresses” section on page 3-21 and the “Permanent Unicast Address Table” section on page 3-29.

Half-Duplex Back Pressure on 10-Mbps Ports

By default, half-duplex back pressure on all 10-Mbps ports is disabled. Back pressure ensures retransmission of incoming packets if a half-duplex 10-Mbps switch port is unable to receive incoming packets.

When back pressure is enabled and no buffers are available to a port, the switch generates collision frames across the affected port and causes the transmitting station to resend the packets. The switch can then use this retransmission time to clear its receive buffer by transmitting packets already in the queue.

For information about flow control on the 100-Mbps ports, see the “Flow Control” section on page 3-20.

ECC on 10-Mbps Ports

By default, enhanced congestion control (ECC) is disabled on all 10-Mbps ports. An ECC-enabled port accelerates transmission of frames and empties its queue more quickly. This option reduces congestion on the switch and keeps the switch from dropping frames because of full transmit queues. The ECC option can be enabled on half-duplex ports and can be configured on a global basis for the 10-Mbps ports.

For information about ECC on the 100-Mbps ports, see the “Enabling or Disabling ECC on the 100-Mbps Ports” section on page 3-22. ECC on the 100-Mbps ports is set on a per-port basis, not on a global basis.

To enable ECC on a 10-Mbps port:

- Step 1** Select one of the following modes from the Enhanced Congestion Control drop-down list.
- **Adaptive**—Causes the port to operate under the ECC Disabled setting if the transmit queue is not full. If the queue is full, the port uses the ECC Aggressive setting.
 - **Disabled**—Causes the port to operate under the standard IEEE 802.3 backoff algorithm for retransmitting frames.
 - **Moderately Aggressive**—Causes the port to use a modified backoff algorithm to more aggressively retransmit frames and empty the queue.
 - **Aggressive**—Is the highest acceleration rate configurable for ECC. The port uses a modified backoff algorithm to more aggressively retransmit frames and empty the queue than when set at ECC Moderately Aggressive.
- Step 2** Click **Apply**.

Broadcast Storm Control

A broadcast storm is an excessive number of broadcast packets being received on a given switch port. Broadcast storm packets can congest the receiving switch port. If the switch port forwards a broadcast storm to the other switch ports, traffic on those ports and all network segments are also affected. You can use broadcast storm control to control the quantity of broadcast packets the switch forwards to your network, thus reserving switch bandwidth for your network users.

Use the broadcast storm control settings to inhibit the forwarding of broadcast packets when the broadcast rate (number of broadcast packets received from a port per second) on a switch port exceeds a specified threshold. Broadcast storm control is configured for the switch as a whole, but operates on a per-port basis.

Note Only broadcast packets are filtered through the broadcast storm control option. For information about unicast and multicast flooding control, see the “Enabling or Disabling Flooding of Unknown MAC Addresses” section on page 3-21 and the “Managing Multicast Packets with CGMP” section on page 3-78.

To change the broadcast storm control settings:

- Step 1** Select **Block** or **Ignore** in the Action Upon Exceeding Broadcast Threshold field. The default is Ignore.
- This option assigns the action the switch takes if the number of broadcast packets reaches the broadcast threshold:
- **Block**—The switch drops all broadcast packets received from a port if the broadcast threshold is exceeded. The switch resumes forwarding if the rate of broadcast packets received drops below the re-enable threshold.
 - **Ignore**—The switch forwards broadcast packets. There is no set threshold.
- Step 2** In the Broadcast Threshold field, enter the threshold that constitutes a broadcast storm. The range is 10 to 14400 broadcast packets received from a port per second. The default is 500.
- When this threshold is exceeded, the switch, if configured to do so, blocks the broadcast packets received from the port and generates an SNMP alert.
- Step 3** In the Broadcast Reenabled Threshold field, enter the threshold below which broadcast forwarding is re-enabled. The range is 10 to 14400 packets. The default is 250.
- Step 4** Click **Apply**.

Managing Multicast Packets with CGMP

A *multicast packet* is information sent to multiple recipients from one sender. However, sometimes multicast traffic needs to be received only on certain networks segments, and not all. Indiscriminant flooding of multicast traffic can waste bandwidth on the switch and congest each segment.

The Cisco Group Management Protocol (CGMP) dynamically creates CGMP groups, which are designated recipients of multicast traffic. This limits the transmission of multicast packets to only end-stations that request them, thereby reducing flooding of multicast traffic within the network.

IP multicast routers are required to forward multicast packets across an IP internetwork. CGMP filtering requires a network connection from a CGMP-enabled switch to a router running CGMP. End stations issue join messages to become part of a CGMP group and issue leave messages to leave the group. A CGMP-enabled router sends CGMP packets to inform the switch when specific end-stations join or leave a CGMP group. When CGMP is enabled on the switch, the switch ports forward multicast traffic only to CGMP group members.

A CGMP group remains in the switch IP Multicast Address Table until all members have left that group. The switch supports up to 64 IP multicast group registrations. For information about multicast registrations, see the “Permanent Multicast Address Table” section on page 3-30.

To display the CGMP Management Page (Figure 3-15), click **CGMP** on the menu bar.

For additional information, see the

- “Permanent Multicast Address Table” section on page 3-30
- “Changing the System Management Settings” section on page 3-68
- “Store-and-Forward for Multicast Frames” section on page 3-74

For information about IP multicast, including Internet Group Management Protocol (IGMP), refer to RFC 1112.

Figure 3-15 CGMP Management Page

HOME PORT ADDRESS SNMP STP CDP SPAN CONSOLE STATISTICS SYSTEM CGMP

Member Switch Host Name: s202-1 Command Switch IP: 10.1.126.35

CGMP Management

Enable CGMP: ☒

Set the switch to use or not use the Cisco Group Management Protocol.

Enable CGMP Fast Leave: ☒

Set the switch to accelerate removal of unused CGMP groups.

Router Hold Time: seconds [5-900 [600]]

Length of time the switch waits for keepalive messages before removing all multicast addresses learned from CGMP.

IP Multicast Address Table:

(none)

Remove

Remove All

Lists the multicasts addresses learned from CGMP.

Router Ports Table:

(none)

Remove

Remove All

Lists the multicast routers learned from CGMP.

26596

Configuring and Monitoring from the Switch Manager 3-79

Changing the CGMP Settings

By default, CGMP is enabled (**Enable CGMP** check box is selected) on the switch.

To disable CGMP:

Step 1 Deselect the **Enable CGMP** check box.

Step 2 Click **Apply**.

CGMP Fast Leave

The CGMP Fast Leave option can eliminate unnecessary multicast traffic to switch ports that no longer have group members needing that specific multicast traffic. By default, the CGMP Fast Leave option is disabled (**Enable CGMP Fast Leave** check box is not selected).

Note For CGMP Fast Leave to take effect, all CGMP group members must have IGMP version 2 enabled.

When this option is enabled, the following rules are in effect:

- If there are no CGMP group members associated with a switch port, the switch disassociates that port from the CGMP group.
- If a CGMP group has no members on any switch port, the CGMP group is removed from the switch IP Multicast Address Table.

To enable CGMP Fast Leave:

Step 1 Select the **Enable CGMP Fast Leave** check box.

Step 2 Click **Apply**.

Router Hold Time

The Router Hold Time field displays the number of seconds (between 5 and 900) that the switch waits for keepalive messages before deleting CGMP-learned multicast groups. By default, the router hold time is 600.

Multicast routers that support CGMP periodically send CGMP join messages to advertise themselves to switches within a network. A receiving switch saves the information and sets a timer equal to the router hold time. The timer is updated every time the switch receives a CGMP join message advertising itself. When the last router hold time expires, the switch removes all IP multicast groups learned from CGMP.

To change the router hold time:

- Step 1** In the Router Hold Time field, specify the number of seconds (5 to 900) the switch waits before removing all IP multicast groups learned from CGMP.
- Step 2** Click **Apply**.

IP Multicast Address Table

When CGMP is enabled on the switch, the switch automatically creates and dynamically maintains a table that lists the addresses of designated multicast recipients and the associated switch port(s) through which multicast traffic are forwarded to those recipients.

If you have configured bridge groups, the bridge group number is not displayed on the IP Multicast Address Table. For more information about bridge groups, see the “Bridge Group Configuration Menu” section on page 4-64.



Caution Use the **Remove** option only to debug and recover from unexpected situations.

To delete a specific entry from the IP Multicast Address Table:

- Step 1** Select the entry you want to delete.
- Step 2** Click **Remove**.

Click **Remove All** to clear the table.

Router Ports Table

CGMP filtering requires a network connection from the switch to a router running CGMP. When CGMP is enabled on the switch, the switch automatically creates and dynamically maintains a table that lists the IP address of each attached CGMP-enabled router and the switch port to which the router is attached.

To delete a specific entry from the Router Ports Table:

Step 1 Select the entry you want to delete.

Step 2 Click **Remove**.

Click **Remove All** to clear the table.