

Web-Based Management

This chapter describes how to use the web console, a GUI for changing the switch configuration and monitoring switch activity. This chapter includes instructions for the most common configuration tasks.

Before continuing with this chapter, you should have read the information in the “Overview of the Web Console” section on page 3-1.

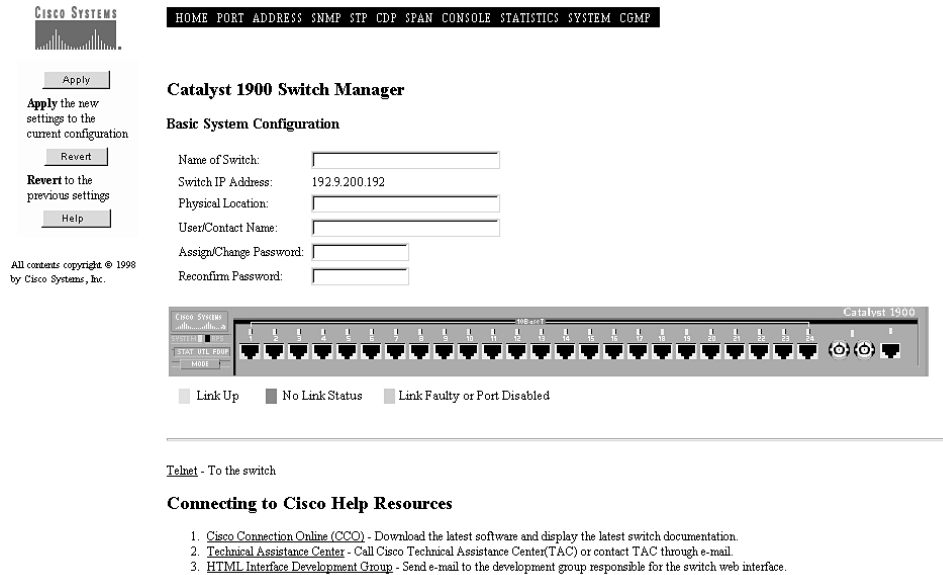
Basic System Configuration Page

To display the Basic System Configuration Page (Figure 4-1), click **Home** on the action bar. You can also display this page by entering the IP address or domain name server of the switch in the URL field, as described in the “Assigning IP Information to the Switch” section on page 2-17. This page acts as the *home* page for the switch web console.

Use this page to:

- Specify basic information about the switch
- Assign or change the password to the switch
- Monitor network activity through the live image of the switch
- Telnet to the switch
- Connect to Cisco help resources

Figure 4-1 Basic System Configuration Page



Entering Basic Configuration Parameters

To operate the switch with its default settings, an IP address must first be assigned to the switch. The IP address is assigned from the [I] option on the Menu Console Logon Screen. The following information (used by network management applications to identify the switch on a network topology map) is also typically assigned but not required.

- Step 1** Enter a name (up to 255 characters) to be used for the switch.
- Step 2** Enter the location (up to 255 characters) of the switch.
- Step 3** Enter the name (up to 255 characters) of the person responsible for the switch.
- Step 4** Click **Apply**.

Entering a New Password or Changing the Password

A switch password is optional. Follow these steps to enter a password:

- Step 1** In the Assign/Change Password field, enter a character string (4 to 8 characters).
- Step 2** In the Reconfirm Password field, reenter the same string.
- Step 3** Click **Apply**.

If a password has already been defined, enter the password at the prompt when you first access the switch using the web console. The Basic System Configuration Page is redisplayed only after you enter the correct password.

If the **Authorization Failed. Retry?** message appears, check that you are using the correct password, and reenter it.

If you have forgotten the password, see the “Recovering from a Lost or Forgotten Password” section on page 6-11.

For information about changing the password, see the “Deleting and Changing the Password to the Switch” section on page 4-39.

Using the Switch Image to Monitor the Switch

This page has an image of the switch that reflects the activity of the LEDs on the switch front panel at the last poll interval. Generally, a green LED means proper functioning, and amber means a problem or malfunction. When an LED is off, the switch or a function is inactive. For information about using the LEDs and the **Mode** button to monitor the switch, see the “LEDs and Mode Button” section on page 1-5.

Using Telnet to Connect to the Switch

Click the **Telnet** hotlink to display the Management Console Main Menu.

Connecting to Cisco Resources

If you need assistance from Cisco, the following resources are available:

- Cisco Connection Online (CCO)—From the CCO Home page, you can display the support sites from where you can, for example, download the latest software and display the latest documentation for the switch.
- Technical Assistance Center—Contact Cisco's Technical Assistance Center (TAC) through e-mail.
- HTML Interface Development Group—Send e-mail to the development group responsible for the switch web interface.

Port Management Page

To display the Port Management Page (Figure 4-2), click **Port** on the action bar, or click the port image on the Basic System Configuration Page. Use this page to:

- Enable or disable fixed ports on the switch
- Display the current status of each fixed port
- Set parameters for the fixed ports
- Display the Detailed Port Statistics report for each fixed port

Figure 4-2 Port Management Page

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 suspended-linkbeat	Half duplex half duplex	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast	Disabled		Stats...
	FastEthernet 0/27	<input checked="" type="checkbox"/> Enable suspended-linkbeat	Full duplex full duplex	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast	Disabled		Stats...

10 Base-T Ports Table:

Module	Port	Status: Requested Actual	Duplex Mode: Requested Actual	Flood Unknown MACs	Port Name/ Description	Statistics
System	Ethernet 0/1	<input checked="" type="checkbox"/> Enable enabled	Half duplex half duplex	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast		Stats...
	Ethernet 0/2	<input checked="" type="checkbox"/> Enable suspended-linkbeat	Half duplex half duplex	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast		Stats...
	Ethernet 0/3	<input checked="" type="checkbox"/> Enable suspended-linkbeat	Half duplex half duplex	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast		Stats...
	Ethernet 0/4	<input checked="" type="checkbox"/> Enable suspended-linkbeat	Half duplex half duplex	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast		Stats...

All contents copyright © 1998 by Cisco Systems, Inc.

11196

Enabling and Disabling a Fixed Port

To enable or disable a port, select or deselect the check box in the Status column, and click **Apply**. The default is Enabled (check box is selected).

To confirm the action, click **Home** on the action bar to display the switch image. The port LED for a disabled port is amber.

Displaying the Current State of a Fixed Port

The current state of each fixed port is shown in the grayed-out field in the Status column. Port status is a system-wide indicator of the state of a port. Security violations, management intervention, or actions of the Spanning-Tree Protocol can change the port status. Each port is always in one of the states listed in Table 4-1:

Table 4-1 Port Status Definitions (Web Console)

Port Status	Definition
Enabled	Port can transmit and receive data.
Disabled-mgmt	Port is disabled by management action. The port must be manually reenabled.
Suspended-no-linkbeat	Suspended due to the absence of a 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	Suspended because attached station is jabbering. Port automatically returns to enabled state when the condition causing the suspension is removed.
Suspended-violation	Suspended due to address violation. Port automatically returns to enabled state when the condition causing the suspension is removed.
Disabled-self-test	Disabled because port failed self-test. Port must be manually enabled.
Disabled-violation	Disabled due to address violation. Port must be manually enabled.
Reset	Port is currently in the reset state.

Changing the Duplex Mode of a Fixed Port

Select the duplex mode from the drop-down menu in the Duplex Mode column for the port, and click **Apply**. The default setting for the 10BaseT ports is half duplex. The default for 100BaseTX ports is autonegotiation-enabled. The default for the 100BaseFX port is half duplex.

Full-duplex operation is simultaneous transmission of data in both directions across a link. For example, 10BaseTX ports operating in full-duplex mode can provide up to 20 Mbps of bandwidth across the switched link. You can use full-duplex connections (either 10 Mbps or 100 Mbps) to enhance transmission speeds between other switches or routers that support full-duplex operation. A likely full-duplex scenario would be to connect a 100BaseT port to a server with a 100BaseT adapter configured for full-duplex operation.

Note As both ends of the link must be configured for full-duplex operation, a full-duplex port cannot be connected to a repeater.

To confirm your changes, follow these steps:

- Step 1** Click **Home** on the action bar to display the image of the switch.
- Step 2** Click the **Mode** button until the FDUP LED lights. If the port status LED is off, the port is running in half duplex. If the port status LED is green, the port is running in full duplex.

If you cannot confirm the actions you requested, return to the Port Management Page and make the changes again.

Enabling and Disabling Flooded Traffic

To enable flooding, select the unicast and multicast check boxes for the port, and click **Apply**. To disable flooding, deselect these check boxes for the port, and click **Apply**.

By default, the switch forwards to all ports (floods) unicast and multicast packets with unknown MAC addresses. As there are some configurations where this flooding is unnecessary, you can disable the flooding of unicast and multicast packets on a per-port basis. To control flooding, the switch forwards, floods, and filters packets in accordance with the IEEE 802.1d specification.

The switch forwards each packet according to the source address stored in the switch address table that matches the destination address of the packet. If the port a packet is received on has both the packet source and destination addresses on it, the packet is filtered (not forwarded).

If the switch cannot match a destination address of a packet with a source address in its address table, the switch floods the packet with the unknown destination address to all ports. Broadcast packets are always flooded to all ports.

For example, when the switch receives a unicast packet with a destination address that it has not learned, the default is to flood it to all ports. On ports with only statically assigned addresses or single stations attached, there are no unknown destinations and flooding would serve no purpose. In this case, you can disable flooding on a per-port basis.

In another example, when the switch receives a multicast packet, you can use the Address Table Management Page or SNMP to register multicast addresses and specify to which ports these packets are to be forwarded. You can also disable the normal flooding of unregistered multicast packets on a per-port basis. Besides reducing unnecessary traffic, these features open up the possibility of using multicast packets for dedicated groupcast applications such as broadcast video.

The switch also supports source-port filtering. This enhanced filtering capability only forwards packets to destinations when they are received on specified ports. These destinations are referred to as restricted static addresses. You can assign restricted static address from the Address Table Management Page.

Enhanced Congestion Control on 100-Mbps Ports

Enhanced congestion control (ECC) helps reduce congestion in the switch and helps keep the switch from dropping frames due to full transmit queues. The default is Disabled.

- Adaptive mode 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 mode causes the port to operate under the standard IEEE 802.3 backoff algorithm for retransmitting frames.
- Moderately Aggressive mode causes the port to use a modified backoff algorithm to more aggressively retransmit frames and empty the queue.
- Aggressive mode 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.

Displaying the Detailed Port Statistics Reports

To display the Detailed Port Statistics Page (Figure 4-3) report on a particular port, click **Stats...** for that port.

Detailed Port Statistics Page

To display the Detailed Port Statistics Page (Figure 4-3), click **Stats...** from the Port Management Page. Use this page to display the receive and transmit port statistics and to help identify performance or connectivity problems, which are indicated under the Errors heading.

Figure 4-3 Detailed Port Statistics Page

Cisco Systems

HOME PORT ADDRESS SNMP STP CDP SPAN CONSOLE STATISTICS SYSTEM CGMP

Detailed Port Statistics

Ethernet 0/1 Statistics Report

Receive Statistics		Transmit Statistics	
Total good frames:	3066	Total frames:	4452
Total octets:	2313057	Total octets:	380261
Broadcast/multicast frames:	43	Broadcast/multicast frames:	1547
Broadcast/multicast octets:	4925	Broadcast/multicast octets:	103028
Good frames forwarded:	3066	Deferrals:	19
Frames filtered:	0	Single collisions:	3
Runt frames:	0	Multiple collisions:	2
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

All contents copyright © 1998 by Cisco Systems, Inc.

11194

Table 4-2 describes the error headings on the page.

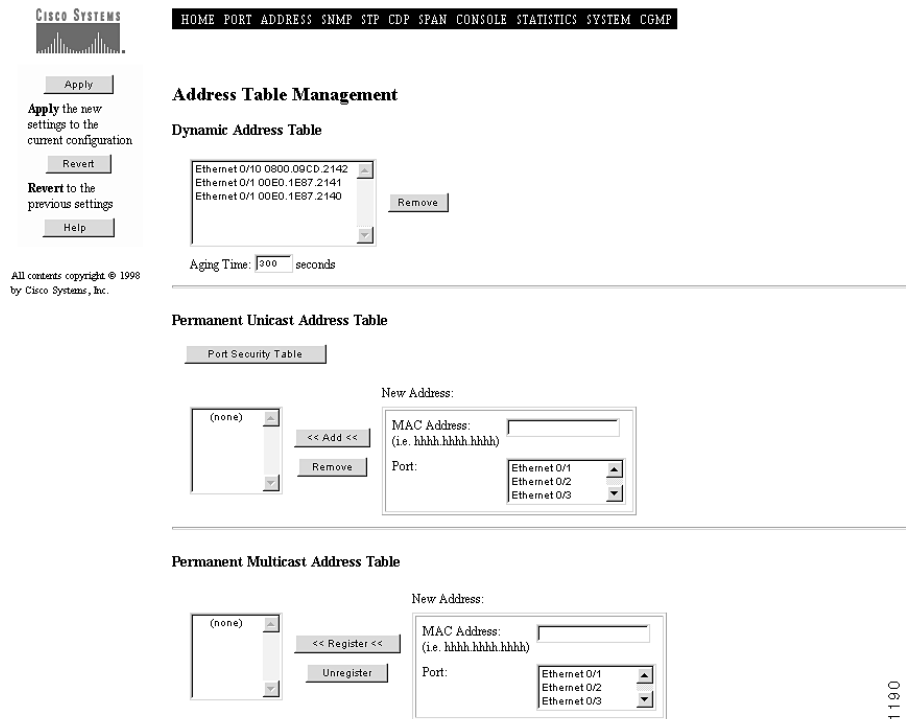
Table 4-2 Error Descriptions on the Detailed Port Statistics Page

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 error	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 secured 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.

Address Table Management Page

To display the Address Table Management Page (see Figure 4-4), click **Address** on the action bar. Use this page to manage the address tables that the switch uses to forward traffic between ports. The address tables list the destination MAC address and the port number. You can also specify how a port filters and forwards unmatched unicast addresses and nonregistered multicast addresses. Although multicast address registrations are configured elsewhere, you can use this menu to specify additional source-port filtering on the multicast addresses.

Figure 4-4 Address Table Management Page



Flooding is the forwarding of unicast and multicast packets with unknown destination addresses to all ports. In certain applications, flooding might be unnecessary and undesirable. To control flooding, the switch forwards, floods, and filters packets in accordance with the IEEE 802.1d specification.

The switch forwards each packet according to the source address stored in the switch address table that matches the destination address of the packet. If the port a packet is received on has both the packet source and destination addresses on it, the packet is filtered (not forwarded).

If the switch cannot match a destination address of a packet with a source address in its address table, the switch floods the packet with the unknown destination address to all ports. Broadcast packets are always flooded to all ports.

For example, when the switch receives a unicast packet with a destination address that it has not learned, the default is to flood it to all ports. On ports with only statically assigned addresses or single stations attached, there are no unknown destinations and flooding would serve no purpose. In this case, you can disable flooding on a per-port basis.

In another example, when the switch receives a multicast packet, you can use the Address Table Management Page or SNMP to register multicast addresses and specify to which ports these packets are to be forwarded. You can also disable the normal flooding of unregistered multicast packets on a per-port basis. Besides reducing unnecessary traffic, these features open up the possibility of using multicast packets for dedicated groupcast applications such as broadcast video.

The switch also supports source-port filtering. This enhanced filtering capability only forwards packets to destinations when they are received on specified ports. These destinations are referred to as restricted static addresses. You can assign restricted static (permanent) addresses from the Address Table Management Page.

Adding and Deleting Dynamic Addresses

To define how long addresses that have not been seen should be retained by the switch, specify in the Aging Time field the number of seconds (10 to 1,000,000) after which an unused dynamic address is automatically removed from the list, and click **Apply**. The default is 300.

To delete an address from the Dynamic Address Table, select the address you want to delete, and click **Remove**.

Dynamic addresses are source Media Access Control (MAC) addresses that are learned by the switch and then dropped when they are not in use. With multiple MAC address support on all ports, you can connect any port on the switch to individual workstations, repeaters, switches, routers, or other network devices. The switch provides dynamic addressing by learning the source address of each packet it receives on each port and adding the address and its associated port number to the address table. As stations are added or removed from the network, the switch updates the address table, adding new entries and aging out those that are currently not in use.

You can manually enter addresses into the address table, including static addresses. Because static addresses do not age, you must manually remove them. Static addressing also allows for a measure of security in that access to a port can be restricted. See the “Port Security Table Page” section on page 4-15 for more information.

Adding and Deleting Permanent Unicast Addresses

To add an address to the table, select the port from the scroll list, specify the MAC address of that port in the MAC Address field, and click **Add**. The address is added immediately to the running (current) configuration and to NVRAM. To delete an address from the table, select the address you want to delete, and click **Remove**.

The Permanent Unicast Address Table contains addresses that an administrator has specifically assigned to certain ports. Unlike dynamic addresses, these addresses are not aged-out. When addressing security is enabled on a port, the permanent addresses statically assigned by an administrator (and possibly other addresses that are *sticky-learned*) determine which hosts can connect to a port. Sticky-learned addresses are learned and made permanent by the switch.

Note Use the procedure in the “Port Security Table Page” section on page 4-15 to secure the port associated with the secure address.

Adding and Deleting Permanent Multicast Addresses

To register an address, select the port from the scroll list, enter the MAC address of that port in the MAC Address field, and click **Register**. To delete an address from the table, select the address you want to delete, and click **Unregister**.

The Permanent Multicast Address Table lists the registered multicast addresses that have been assigned to each port on the switch.

Port Security Table Page

To display the Port Security Table Page (Figure 4-5), click **Port Security Table** from the Address Table Management Page. Use this page to enable port security on a port and to define the size of the address table for secured ports.

Limiting the number of devices that can connect to a secure port can have 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.

The following fields validate port security or indicate security violations:

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

Note Security is checked against the SRC addresses of incoming packets.

Figure 4-5 Port Security Table Page

Port Security Table

Module	Port	Security	Maximum Secure Addresses	Security Reject Count
system	Ethernet 0/1	<input type="checkbox"/>	0	N/A
	Ethernet 0/2	<input type="checkbox"/>	0	N/A
	Ethernet 0/3	<input type="checkbox"/>	0	N/A
	Ethernet 0/4	<input type="checkbox"/>	0	N/A
	Ethernet 0/5	<input type="checkbox"/>	0	N/A
	Ethernet 0/6	<input type="checkbox"/>	0	N/A
	Ethernet 0/7	<input type="checkbox"/>	0	N/A
	Ethernet 0/8	<input type="checkbox"/>	0	N/A
	Ethernet 0/9	<input type="checkbox"/>	0	N/A
	Ethernet 0/10	<input type="checkbox"/>	0	N/A
	Ethernet 0/11	<input type="checkbox"/>	0	N/A
	Ethernet 0/12	<input type="checkbox"/>	0	N/A
	Ethernet 0/13	<input type="checkbox"/>	0	N/A
	Ethernet 0/14	<input type="checkbox"/>	0	N/A
	Ethernet 0/15	<input type="checkbox"/>	0	N/A
	Ethernet 0/16	<input type="checkbox"/>	0	N/A
	Ethernet 0/17	<input type="checkbox"/>	0	N/A
	Ethernet 0/18	<input type="checkbox"/>	0	N/A
	Ethernet 0/19	<input type="checkbox"/>	0	N/A
	Ethernet 0/20	<input type="checkbox"/>	0	N/A
	Ethernet 0/21	<input type="checkbox"/>	0	N/A

Securing a Port

To enable port security on a port, select the check box in the Security column, and click **Apply**. The default is Disabled (check box is not selected).

On the following web console pages, you can specify the action the switch takes when 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.

Defining the Maximum Secure Address Count

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

Enter a number from 1 to 132 in the Maximum Secure Addresses column, and click **Apply**.

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

The number of devices on a secured port can range from 1 to 132. The addresses for the devices on a secure port are statically assigned by an administrator or *sticky-learned*. Sticky-learning takes place when the address table for a secured 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.

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

- When the address table of a secured port is full and the address of an incoming packet is not found in the table
- When an incoming packet has a source address statically assigned to another port

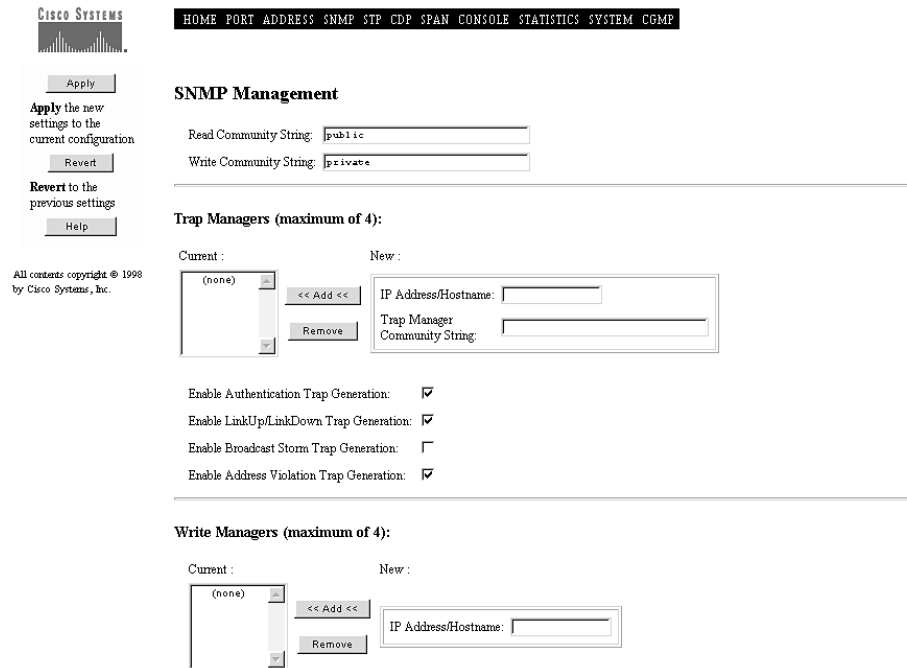
When a security violation occurs, the port can be suspended or disabled. When a port is disabled, you must manually reenab the port. When a port is suspended, it is reenabled when a packet containing a valid address is received. You can also choose to ignore the violation and keep the port enabled. You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

SNMP Management Page

To display the SNMP Management Page (see Figure 4-6), click **SNMP** on the action bar. Use this page to perform the following tasks:

- Entering SNMP read and write community strings
- Enabling and disabling trap generation
- Defining trap manager settings
- Defining write manager settings

Figure 4-6 SNMP Management Page



11188

You can use SNMP management, based on the Catalyst 1900 MIB, to specify management stations authorized to set configuration parameters and to receive traps. Up to four management stations can set MIB objects, and up to three stations can receive traps. If no

management station is specified, any SNMP station can set parameters if the correct write community string accompanies the request. However, once a write-manager IP address is defined, only an explicitly specified management station can issue set operations. Once a management station has been assigned, it receives all traps issued by the switch.

Entering the SNMP Community Strings

Community strings serve as passwords for SNMP messages.

To define the SNMP agent read community string, enter up to 32 characters in the Read Community String field, and click **Apply**. The default is Public.

To define the write community string for the switch, enter up to 32 characters in the Write Community String field, and click **Apply**. The default is Private.

Enabling and Disabling Trap Generation

To enable or disable trap generation, use the following check boxes, and click **Apply**.

- Enable Authentication trap generation—If this check box is selected, authentication traps alert a management station of SNMP requests not accompanied by a valid community string. Even if this parameter is set, no trap can be generated if no trap manager addresses have been specified. The default is Enabled (check box is selected).
- Enable LinkUp/LinkDown trap generation—If this check box is selected, the switch generates the linkDown trap 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)
 - User disabling the port

The linkUp trap is generated when a port is enabled for any of these reasons:

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

The default is Enabled (check box is selected).

- Enable Broadcast Storm trap generation—If this check box is selected, the switch generates SNMP alerts when the broadcast threshold is exceeded. The default is Disabled (check box is not selected).
- Enable Address Violation trap generation—If this check box is selected, the switch generates SNMP alerts when the address violation threshold is exceeded. The default is Enabled (check box is selected).

Defining Trap Manager Settings

A trap manager, or trap client, is a management workstation configured to receive and process traps. You can enter up to four trap managers and their accompanying community strings. Enter the IP address or host name and community string in the IP Address/Hostname and Community String fields, and click **Add**. To delete a manager from the Trap Manager scroll list, select the trap manager, and click **Remove**.

A trap manager community string can contain 32 characters. You can specify the IP address for the trap manager in dotted quad format (nnn.nnn.nnn.nnn). You can specify the name of the trap manager if the switch is connected to a domain name server.

Continue with further definitions for the second, third, and fourth traps, as needed.

For more information about traps, see the “Using FTP to Access the MIB Files” section on page 3-15.

Defining Write Manager Settings

Up to four IP addresses or host names of stations can issue write requests to the switch. Enter the IP address or host name of that station in the IP Address/Hostname field, and click **Add**. To delete a manager from the Write Manager scroll list, select the write manager, and click **Remove**.

Spanning-Tree Management Page

To display the Spanning-Tree Management Page (Figure 4-7), click **STP** on the action bar. Use this page to change parameters for the Spanning-Tree Protocol (STP), an industry standard for avoiding loops in switched networks. The first part of the page displays the current spanning-tree operating parameter values received from the root bridge, spanning-tree settings for the current root switch, and the settings this switch is to use when it becomes the root switch. The second part of this page is used to define port-level parameters.

Figure 4-7 Spanning-Tree Management Page

Spanning-Tree Management

Enable Spanning Tree:

Spanning Tree Operating Parameters

Bridge ID: 8000.00E0.1E7E.BE80 Designated Root: 8000.00E0.1E7E.BE80
 Number of Member Ports: 27 Root Port: 0
 Max Age: 20 seconds Root Path Cost: 0
 Hello Time: 2 seconds Forward Delay: 15 seconds
 Topology Changes: 0 Last TopChange: 0a00h00m00s

Spanning Tree Configurations

Bridge Priority: Max Age: seconds
 Hello Time: seconds Forward Delay: seconds

Port Parameters

Module	Port	State	Forward Transitions	Path Cost	Priority	Port Fast Mode
	Ethernet 0/1	Forwarding	1	100	128	<input checked="" type="checkbox"/> Enable
	Ethernet 0/2	Blocking	0	100	128	<input checked="" type="checkbox"/> Enable
	Ethernet 0/3	Blocking	0	100	128	<input checked="" type="checkbox"/> Enable
	Ethernet 0/4	Blocking	0	100	128	<input checked="" type="checkbox"/> Enable
	Ethernet 0/5	Blocking	0	100	128	<input checked="" type="checkbox"/> Enable
	Ethernet 0/6	Blocking	0	100	128	<input checked="" type="checkbox"/> Enable
	Ethernet 0/7	Blocking	0	100	128	<input checked="" type="checkbox"/> Enable
	Ethernet 0/8	Blocking	0	100	128	<input checked="" type="checkbox"/> Enable

11201

Enabling and Disabling Spanning-Tree Protocol

Spanning-Tree Protocol is enabled by default (check box is selected). To disable Spanning-Tree Protocol, deselect **Enable Spanning Tree**, and click **Apply**.

Note Modifying the spanning-tree settings results in a temporary loss of connectivity while the network reconfigures.

Spanning-Tree Operating Parameters

The following parameters are read-only and could be defined on another switch.

- **Bridge ID**—Unique hexadecimal ID number has a bridge priority and a unique MAC address.
- **Number of Member Ports**—Number of ports configured with Spanning-Tree Protocol.
- **Max Age**—Number of seconds a bridge waits without receiving Spanning-Tree Protocol configuration messages before attempting a reconfiguration.
- **Hello Time**—Number of seconds between the transmission of Spanning-Tree Protocol configuration messages. All bridges send configuration messages during reconfiguration to elect the designated root bridge. After the topology is stabilized, only designated bridges send configuration messages.
- **Topology Changes**—Number of bridge topology changes experienced by this bridge. A topology change occurs as ports on this bridge change from a nonforwarding to forwarding state or when a new root is selected.
- **Designated Root**—ID of the bridge identified as the root by the Spanning-Tree Protocol.
- **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 Spanning-Tree Protocol 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 Designated root. It equals the path cost parameters held for the root port. When this switch is the root, the root path cost is zero.

- Forward Delay—Number of seconds before a port changes from its Spanning-Tree Protocol learning and listening states to a forwarding state. This is necessary because every bridge on the network ensures no loop is formed before allowing the port to forward packets.
- Last TopChange—Number of days (d), hours (h), minutes (m), and seconds (s) since the last topology change.

Changing Spanning-Tree Configurations for the Bridge

To change the spanning-tree parameters that this switch would use as the root switch, change the following parameters, and click **Apply**.

Note You can only configure the STP parameters for bridge group 1, the management bridge group. For more information about bridge groups, see the “Bridge Group Configuration Menu” on page 47.

- Priority—Value (0 through 65535) used in determining the identity of the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. The default is 32768.
- Hello Time—Number of seconds (1 to 10) when this switch becomes the root bridge. The default is 2.
- Max Age—Number of seconds (6 to 40) to be used as the Max age interval when this switch becomes the root bridge. 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.
- Forward Delay—Number of seconds (4 to 30) to be used as the forward-delay interval when this switch becomes the root bridge. The default is 15.

Changing Spanning-Tree Parameters for a Port

To change the spanning-tree parameters for a port, change the following parameters, and click **Apply**.

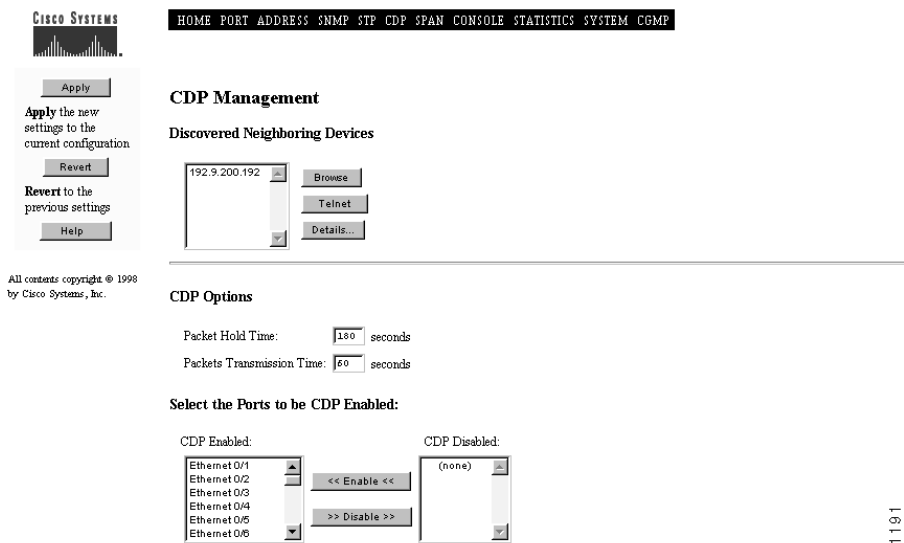
- State—Displays the spanning-tree state of the port:
 - Blocking: Port is not participating in the frame-forwarding process and is not learning new addresses.
 - Listening: The same as blocking, but the switch is actively trying to bring the port into the forwarding state. The port is not learning addresses.
 - Learning: Port is not forwarding frames but is learning addresses. The switch is trying to change the port to the forwarding state.
 - Forwarding: Port is forwarding frames and learning addresses.
 - Disabled: Port has been removed from operation. Administrative intervention is required to enable the port.
- Forward transitions—Number of times Spanning-Tree Protocol changed forwarding states. An increase in this number might indicate that Spanning-Tree Protocol detected a network loop.
- Path Cost—Spanning-Tree Protocol path cost (1 to 65,535) of the port. It 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. The default is 100.
- Priority—The port (0 to 255) remains enabled by Spanning-Tree Protocol if two ports to another switch form a loop. The default for 10BaseT ports is 128; default for 100BaseT ports is 10.
- Port Fast Mode—Select this check box to accelerate the time it takes for Spanning-Tree Protocol to bring a port into the forwarding state by immediately transitioning from blocking to forwarding. Port Fast-enabled ports should only be used for end-station attachments. The default for 10BaseT ports is Enabled (check box is selected). The default for 100BaseT ports is Disabled (check box is not selected).

CDP Management Page

To display the CDP Management Page (see Figure 4-8), click **CDP** on the action bar. Use this page to enable CDP for the switch, set the global CDP parameters, and display information about neighboring devices.

Cisco Discovery Protocol (CDP) is a device-discovery protocol that the switch uses to maintain information about neighboring devices. Network-management applications that support CDP can then use this information to discover those devices. By gathering information about the types of devices in the network, the links between those devices, and the number of interfaces within each device, CDP enables network management applications to display a topological map of the network. Detailed information about the connections between devices is also available.

Figure 4-8 CDP Management Page



Listing and Displaying Neighboring Devices

The CDP Neighbors list shows the devices with which this switch is exchanging CDP messages.

To browse a specific neighbor from the web console, the neighbor must be a device that has web-console support. Select the neighbor from the scroll list, and click **Browse**.

To Telnet to a neighbor, the neighbor must have Telnet support. Select the neighbor from the scroll list, and click **Telnet**.

To display detailed information about a neighbor, select it from the scroll list, and click **Details...**

Setting CDP Options

In the Packet Hold Time field, specify the number of seconds (5 to 255) that the switch keeps the CDP neighbor information, and click **Apply**. The default is 180.

In the Packet Transmission Time field, specify the number of seconds (5 to 900) between CDP messages, and click **Apply**. The default is 60.

Note All ports are subject to the parameters under the heading CDP Options.

Enabling CDP on Ports

To enable CDP on one or more ports, select the port from the CDP Disabled scroll list, and click **Enable**.

There can be times when you do not want CDP to exchange information with certain devices. In this case, disable the port with the devices attached to it. To disable CDP on a port, select the port you want to delete from the CDP Enabled scroll list, and click **Disable**.

Note Only 15 ports can be enabled or disabled at a time.

SPAN Configuration Page

To display the SPAN Configuration Page (Figure 4-9), click **SPAN** on the action bar. Use this page to do the following:

- Turn frame capturing on and off
- Define those ports whose frames are to be captured
- Define the port to where the captured frames are to be sent

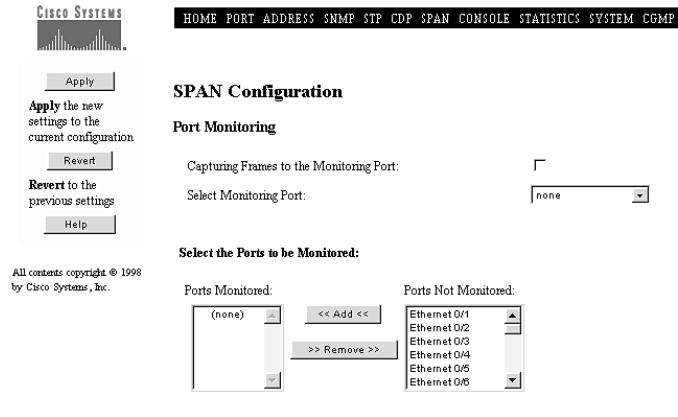
Frame capturing cannot take place until all three of these parameters have been set.

You can route a copy of incoming and outgoing port traffic to a monitor port for analysis and troubleshooting. When a port is selected as the monitor port, it sends out only traffic seen on the ports defined in the port capture list.

Note Spanning-Tree Protocol and BOOTP are disabled on the enabled monitor port. The flooding of unregistered multicast packets and unknown unicast packets is similarly inhibited.

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

Figure 4-9 SPAN Configuration Page



11199

You can monitor traffic on a given port by forwarding incoming and outgoing traffic on the port to another port. Any port can be defined as the monitor port, and any combination of ports can be monitored.

To enable port monitoring, change the following parameters, and click **Apply**.

To enable frame capturing on the monitoring port, select the Capturing frames to the Monitor check box, and click **Apply**. The default is Disabled (check box is not selected).

Select the port to which captured frames are to be sent, and click **Apply**. The default is None.

To select ports to be monitored, select the port listed in the Ports Not Monitored scroll list, and click **Add** to move to the ports to the Ports Monitored scroll list.

To remove ports from the Ports Monitored scroll list, select the ports you want to remove from the Ports Monitored scroll list, and then click **Remove**.

Note Only 15 ports can be selected at a time.

Console and Upgrade Configuration Page

To display the Console and Upgrade Configuration Page (Figure 4-10), click **Console** on the action bar. Use this page to set the console port parameters and to upgrade the switch firmware.

Figure 4-10 Console and Upgrade Configuration Page

Console and Upgrade Configuration

Console

Baud Rate: 9600 baud

Data Bits: 8 bit(s)

Stop Bits: 1 bit(s)

Parity Setting: None

Management Console Inactivity Timeout: 0

Initialization String for Modem:

Enable Auto Baud (Match Remote Baud Rate):

Enable Auto Answer:

Firmware Upgrade Options

Firmware Version: V8.00.00(21) written from serial terminal

Server IP Address or Name of TFTP Server:

Filename for Firmware Upgrades:

Accept Upgrade Transfer from Other Hosts:

System TFTP Upgrade

Apply
Apply the new settings to the current configuration

Revert
Revert to the previous settings

Help

All contents copyright © 1998 by Cisco Systems, Inc.

11193

Configuring the Console Port

After connecting the console port of the switch to a management station or modem, set the following default characteristics of the console port to match the characteristics of the management station or modem, and click **Apply**.

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

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

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

Set the following parameters to define the call features, and click **Apply**:

- Management Console inactivity timeout—Number of seconds (30 through 65,500) the management console is idle before timing out and logging you out. After timeout, you must re-enter the password. The default is 0 (management console never times out).
- Initialization string for modem—String to be used by the switch to initialize the modem connected to the console port. This string must match your modem requirement. Do not use an AT prefix or end-of-line suffix.
- Enable auto baud (match remote baud rate)—When this check box is selected, the switch automatically matches the same or lower baud rate of an incoming call. After the call, the switch reverts to its configured rate. The default is Enabled (check box is selected).
- Enable auto answer—When this check box is selected, the switch automatically answers calls. The default is Enabled (check box is selected).

Upgrading the Switch Firmware

The Switch Version field displays the firmware version currently used by the switch. You can download the latest switch firmware from a TFTP server or from a TFTP client.

Note After the download, the switch does not respond to commands for approximately 1 minute. The switch then resets and begins using the new firmware.

To download the switch firmware from a TFTP server, follow these steps:

- Step 1** Enter the IP address or name of the TFTP server in the Server: IP Address or Name of TFTP Server field.
- Step 2** Enter the upgrade file name in the Filename for Firmware Upgrades field.
- Step 3** Click **System TFTP Upgrade** to download the upgrade file from the TFTP server to the switch.

To download the switch firmware from a TFTP client, follow these steps:

- Step 1** Select **Accept Upgrade Transfer from Other Hosts**.

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

- 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** 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**).

Statistics Reports Page

To display the Statistics Reports Page (Figure 4-11), click **Statistics** on the action bar. Use this page to reset the statistics of all ports and to display the summary exception and utilization statistics.

Figure 4-11 Statistics Reports Page

Statistics Reports

Select Port:

Exception Statistics Report (frame counts):

Port	Receive Errors	Transmit Errors	Port	Receive Errors	Transmit Errors
Ethernet 0/1	0	0	Ethernet 0/15	0	0
Ethernet 0/2	0	0	Ethernet 0/16	0	0
Ethernet 0/3	0	0	Ethernet 0/17	0	0
Ethernet 0/4	0	0	Ethernet 0/18	0	0
Ethernet 0/5	0	0	Ethernet 0/19	0	0
Ethernet 0/6	0	0	Ethernet 0/20	0	0
Ethernet 0/7	0	0	Ethernet 0/21	0	0
Ethernet 0/8	0	0	Ethernet 0/22	0	0
Ethernet 0/9	0	0	Ethernet 0/23	0	0
Ethernet 0/10	0	0	Ethernet 0/24	0	0
Ethernet 0/11	0	0	Ethernet 0/25	0	0
Ethernet 0/12	0	0	FastEthernet 0/26	0	0
Ethernet 0/13	0	0	FastEthernet 0/27	0	0
Ethernet 0/14	0	0			

All contents copyright © 1998 by Cisco Systems, Inc.

Utilization Statistics Report:

Port	Receive	Forward	Transmit	Port	Receive	Forward	Transmit
Ethernet 0/1	3201	3201	4692	Ethernet 0/15	0	0	0

11200

Resetting Port Statistics

To reset statistics for a port, select the port from the Selected Port scroll list, and click **Reset Port Statistics**.

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

Displaying the Exception Statistics Report

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

- Receive—Combined number of giants, FCS, and alignment errors
- Transmit—Combined number of excessive deferrals, late collisions, jabber errors, and other transmit errors

Displaying the Utilization Statistics Report

This report displays the number of frames received, forwarded, and transmitted for each port.

- Receive—Number of received unicast frames, multicast frames, and broadcast frames
- Forward—Number of good frames forwarded
- Transmit—Combined number of transmitted unicast frames, multicast frames, and broadcast frames

System Management Page

To display the System Management Page (Figure 4-12), click **System** on the action bar. Use this page to define the switch system-wide parameters and configure broadcast storm control.

Figure 4-12 System Management Page

All contents copyright © 1998 by Cisco Systems, Inc.

11202

Assigning IP Information

After you set the following IP parameters for the switch, click **Apply**:

- **IP Address**—Automatically displayed on this page. The IP address is first assigned from the [I] IP Address option on the Menu Console Logon screen. Therefore, on this page, the IP Address of the switch is automatically displayed in the field and should be treated as read-only. If you decide to change it from this page and click **Apply**, the new IP address takes effect immediately.

Note Changing the IP address from this page could cause you to lose connectivity with the switch.

- **Subnet mask**—IP address of the switch if IP subnetting is used. If subnetting is not used, it is the same as the network mask.
- **Domain name**—Name of the DNS domain to which the switch is associated (such as cisco.com).
- **Default gateway**—For SNMP management, default gateway router address used when the switch is trying to reach a nonlocal IP host. This field is filled automatically when the Routing Information Protocol finds a router connected to a port on the switch.
- **IP Address of DNS Servers 1 and 2**—IP addresses of the domain name system servers.
- **Use Routing Information Protocol**—If this check box is selected, the switch automatically discovers IP gateways. The default is Enabled (check box is selected).

Assigning Switch Parameters

To improve switch performance and set flood or traffic control, set the following parameters, and click **Apply**:

- **Switching mode**—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 filters out collision fragments before forwarding. Store-and-forward stores complete packets and checks for errors before forwarding. The default is FragmentFree.

The switch offers the following switching modes:

- The default mode, FragmentFree, is a form of *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.

- The store-and-forward 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 100 Mbps, the packet receipt time varies between 51.2 microseconds and 1.2 milliseconds. At 10 Mbps, the packet receipt time varies between 5.12 and 120 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 (see Table 4-3). 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.

Table 4-3 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 ¹	7 microsec	7 microsec	3 microsec	3 microsec

1. Although this table 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.

- **Enable the Use of Store-and-Forward for Multicast**—If this check box is selected, the switch uses store-and-forward for multicast frames. If it is not selected, multicast frames are handled according to the switching mode. The default is Disabled (check box is not selected).
- **Action Upon Address Violation**—Occurs if a secured port receives a source address statically assigned to another port or if a secured port tries to learn more than a defined number of addresses. The default is Suspend.
 - Suspend causes the port to stop forwarding until a packet with a valid source address is received.
 - Disable disables the port. The port is permanently disabled and requires user-intervention to be enabled.
 - Ignore causes the port status to remain unchanged.
- **Network Port**—The destination port for all packets with unknown unicast addresses. The default is None. The network port:
 - Does not learn addresses.
 - Is usually connected to a legacy network or backbone.
 - Cannot be a secured port.
 - Cannot be port A or B if Fast EtherChannel mode or trunking is enabled (Enterprise Edition software-specific).

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 address from its memory, 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.

- **Half-Duplex Back Pressure for All 10-Mbps Ports**—Back pressure ensures retransmission of incoming packets when a 10-Mbps port, configured for half-duplex operation, is temporarily unable to receive incoming frames. The default is Disabled.

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.
- **Enhanced Congestion Control for All 10-Mbps Ports**—Enhanced congestion control (ECC) helps reduce congestion in the switch and helps keep the switch from dropping frames due to full transmit queues. The default is Disabled.
 - 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.

Deleting and Changing the Password to the Switch

If a password has been defined, and you want to delete it, click **Clear Password**.

If you want to change the password, click **Clear Password**. Then, from the Basic System Configuration Page (the Home page), follow these steps:

- Step 1** Enter a character string (4 to 8 characters) in the Assign/Change Password field.
- Step 2** Enter the same character string in the Reconfirm Password field, and click **Apply**.

Configuring Broadcast Storm Control

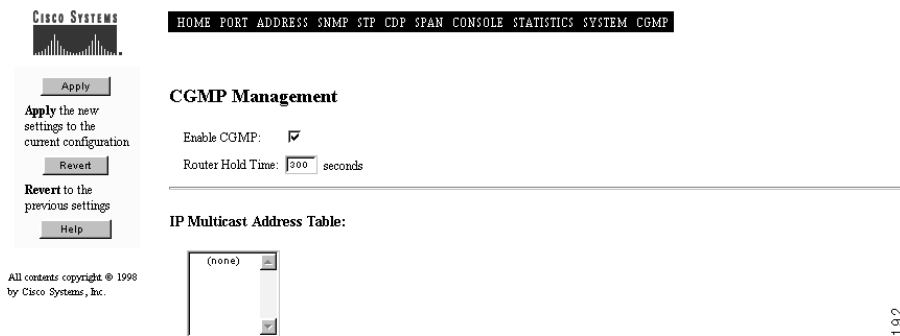
To inhibit the forwarding of broadcast packets when an excessive number of them arrive from a given port, change the following settings, and click **Apply**:

- Action upon exceeding broadcast threshold—Action the switch takes when the number of broadcast packets reaches the broadcast threshold. When blocking, the switch drops all broadcast packets received from a port when the rate of broadcast packets exceeds the threshold. Forwarding resumes when the rate of broadcast packets received drops below the reenabled threshold. The default is Ignore.
- Broadcast threshold—Number of packets per second (10 to 14,400) arriving on a port. When this threshold is exceeded, the switch blocks the forwarding of packets on the port and generates an SNMP alert, if configured to do so. The broadcast rate is the number of broadcast packets received from a port in 1 second. If the broadcast rate exceeds the specified threshold and broadcast storm control is enabled, the switch generates an alert or block broadcast packets received from the port. The default is 500.
- Broadcast reenabled threshold—Number of broadcast packets received from a blocked port must drop below this threshold (10 to 14,400) before packet forwarding resumes. The default is 250.

CGMP Management Page

To display the CGMP Management Page (Figure 4-13), click **CGMP** on the action bar. Use this page to enable Cisco Group Management Protocol (CGMP) and list the IP multicast addresses currently being handled by CGMP.

Figure 4-13 CGMP Management Page



11192

CGMP reduces the unnecessary flooding of IP multicast packets by limiting the transmission of these packets to only the CGMP clients that should receive them. CGMP manages multicast traffic by allowing directed switching of IP multicast traffic within a network. CGMP offers the following benefits:

- Allows IP multicast packets to be switched only to those ports that have IP multicast clients.
- Saves network bandwidth on user segments by not propagating unnecessary IP multicast traffic.
- Does not require changes to the end host systems.

CGMP filtering requires a network connection from the switch to a router running CGMP. When CGMP is enabled, it automatically identifies the ports to which the CGMP-capable router is attached. CGMP is enabled by default and supports a maximum of 64 IP multicast group registrations.

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

For additional information about CGMP and multicast addresses, see the “System Management Page” section on page 4-34 and the “Address Table Management Page” section on page 4-12.

Enabling CGMP

To enable CGMP, select the check box, and click **Apply**. The default is Enabled (check box is selected).

Modifying the Router Hold Time

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, and click **Apply**. The default is 300.

The Router Hold Time field displays the number of seconds (between 5 and 900) the switch waits for keepalive messages before deleting CGMP-learned multicast groups. 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 CGMP-capable router goes down, the switch discards the multicast-group information from the router.

Listing IP Multicast Addresses

The IP Multicast Address Table lists the IP multicast addresses currently controlled by CGMP and the destination ports that will receive multicast traffic to this address.

