CHAPTER 4

Configuring and Monitoring from the Management Console

This chapter explains how to use the management console to change the configuration settings and to monitor the switch. This chapter assumes that you have already performed the following 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 Management Console and CLI" section on page 2-41

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*.

The menus and displays in this chapter are for reference only and might not exactly reflect the menus and displays on your console.

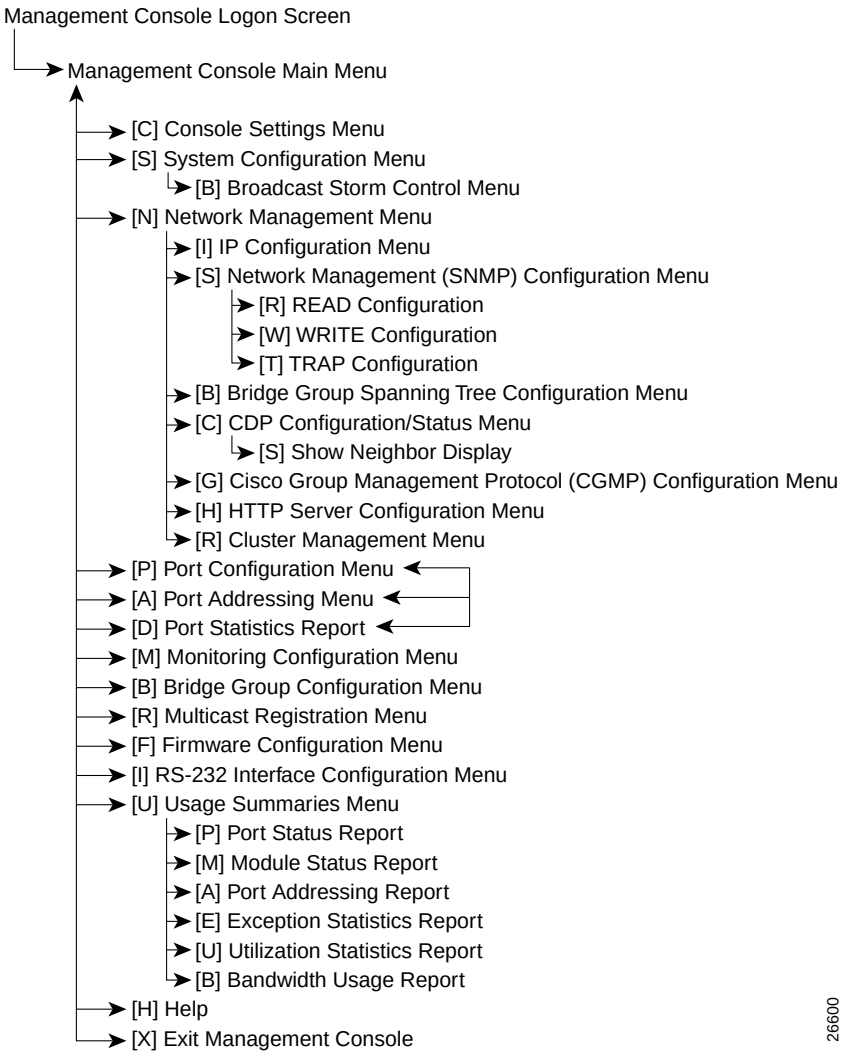
Navigating the Management Console

Figure 4-1 lists the menus that are available from the Main Menu of the management console.

To select an option, enter a letter in the Enter Selection field. You do not need to press **Return**.

To return to a parent menu, enter [**X**] Exit. To exit the management console and return to the command prompt, enter [**X**] Exit on the Management Console Logon Screen.

Figure 4-1 Management Console Menus and Displays



Making Changes from the Management Console

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.

Press **Return** to save changes.

The information you enter at the prompts is not case sensitive, except when entered as a descriptive string that preserves case. Press the **Backspace** key to erase characters you enter. To clear an entry, place the cursor at the beginning of an entry, and press **Backspace**.

To cancel your unsaved changes, place the cursor at the beginning of an entry, and press **Return**. The menu is redisplayed unchanged.

When you use the management console, keep the following in mind:

- You can restrict access to the management console by using a password and locking out a user who fails to enter the password within a set number of attempts. The network administrator can then be alerted by in-band management messages. For information about passwords, see the “Console Settings Menu” section on page 4-6.
- Menus display the current settings used by the switch except when parameters are activated as a group. In certain cases, the settings are overridden by the settings on some menus and become active when those settings are turned off.
- Certain menus, such as the RS-232 Port Configuration Menu, allow activation of the given parameters as a group.

Note If you are using VT100 terminal emulation, the statistics displayed from the management console are refreshed every 5 seconds. If you are connected to the management console through a modem running at less than 2400 baud, the statistics displays are refreshed every 8 seconds. Press **Return** or the **Spacebar** to refresh these reports at any time.

Management Console Logon Screen

The Management Console Logon Screen (Figure 4-2) is displayed on the management station after you connect to the switch through the console port or through a Telnet session. (For complete information about the console port, see the "Connecting to the Console Port" section on page 2-16. For information about logging on to the management console, see the "Accessing the Management Console and CLI" section on page 2-41.)

Figure 4-2 Management Console Logon Screen

```
Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc.  1993-1999
All rights reserved.

Standard Edition Software
Ethernet address:      00-E0-1E-7E-B4-40

PCA Number: 73-2239-01
PCA Serial Number: SAD01200001
Model Number: WS-C1924-A
System Serial Number: FAA01200001
--------------------------------------

      User Interface Menu

      [M] Menus
      [I] IP Address
      [P] Console Password

Enter Selection:
```

Note Even if the switch has an IP address, the [I] IP Address and [P] Console Password options are displayed if a switch password has not been assigned.

[M] Menus—Display the Management Console Main Menu.

[I] IP Address—Display the IP Configuration Menu. This option is available at log on only if the switch does not have a password. For information about IP addresses, see the "IP Configuration Menu" section on page 4-20.

[P] Console Password—Enter a 4-to-8 character unencrypted privileged-level password to the switch management interfaces. This option is available at log on only if the switch does not have a password. For information about passwords, see the "Changing the Switch Password" section on page 4-8.

Management Console Main Menu

To display the Management Console Main Menu (Figure 4-3), enter the **[M] Menus** option from the Management Console Logon Screen. To select an option from the menu, enter a letter in the Enter Selection field. You do not need to press **Return**.

The remaining sections in this chapter describe the options available from this menu.

Figure 4-3 Management Console Main Menu

```
Catalyst 1900 - Main Menu

[C] Console Settings
[S] System
[N] Network Management
[P] Port Configuration
[A] Port Addressing
[D] Port Statistics Detail
[M] Monitoring
[B] Bridge Group
[R] Multicast Registration
[F] Firmware
[I] RS-232 Interface
[U] Usage Summaries
[H] Help

[X] Exit Management Console

Enter Selection:
```

[H] Help—Display the online help and to change the expertise level of the online prompts.

Note If the switch is running the Cisco Catalyst 1900/2820 Enterprise Edition Software and the VLANs option is enabled, the [V] Virtual LAN option replaces the [B] Bridge Group option on the Management Console Main Menu. This chapter describes standard-edition options only. 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*.

Console Settings Menu

To display the Console Settings Menu (Figure 4-4), enter the **[C] Console Settings** option from the Management Console Main Menu.

Figure 4-4 Console Settings Menu

```
Catalyst 1900 - Console Settings

--------------------Settings------------------
[P] Password intrusion threshold               3 attempt(s)
[S] Silent time upon intrusion detection       None
[T] Management Console inactivity timeout      None
[D] Default mode of status LED                 Port Status

--------------------Actions-------------------
[M] Modify password
[E] Modify secret password

[X] Exit to Main Menu

Enter Selection:
```

[P] Password intrusion threshold—Enter the allowed number of failed password attempts. After this number is reached, the management console becomes quiet for a user-defined length of time (see the [S] Silent time upon intrusion detection option) before allowing the next log-in attempt. The default is 3.

[S] Silent time upon intrusion detection—Enter the number of minutes (0 to 65500) the management console is unavailable because of an excessive number of failed attempts to log in. The default is None (no silent time).

[T] Management console inactivity time-out—Enter the number of seconds (0, or a number between 30 and 65500) the management console can wait without activity before it times out. After timeout, you must reenter the password. The default is 0, which means the console session does not time out.

[D] Default mode of status LED—Select the default mode of the port LEDs (see the "Port LEDs and Modes" section on page 1-8). The switch returns to this mode 30 seconds after you release the Mode button. You can enter [**1**] Port Status, [**2**] Utilization, or [**3**] Duplex Status. The default is [1] Port Status.

[M] Modify password—Enter the unencrypted privileged-level password for the switch management interfaces. The password can be 4 to 8 characters and *is not 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.

Note Unlike assigning a password through the CLI, do not enclose a multistring password within double-quotation marks unless you intend for the quotation marks to be part of the password (such as "*two words"*).

If the switch already has a password, you must enter it before it can be changed. To erase a password, press the **Backspace** key, and then press **Return**. The default is None.

For more information about passwords, see the "Changing the Switch Password" section on page 4-8.

[E] Modify secret password—Enter the encrypted (secret) privileged-level password for the switch management interfaces. 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.

If the switch already has a password, you must enter it before it can be changed. To erase a password, press the **Backspace** key, and then press **Return**. The default is None.

For more information about passwords, see the "Changing the Switch Password" section on page 4-8.

[X] Exit—Display the Management Console Main Menu.

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).

If you had assigned a password from the [P] Console Password option on the Management Console Logon Screen (see the "Assigning IP Information and a Password to the Switch" section on page 2-19), that password is an unencrypted privileged-level password.

From the Console Settings Menu, you can either use the [M] Modify password option to assign an unencrypted password or use the [E] Modify secret password option to assign an encrypted (secret) privileged-level password. An encrypted 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 or [M] Modify password options. (For more information about where you can assign privileged-level passwords, see the "Privileged-Level Passwords" section on page 4-9.)

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 Password" section on page 4-10.

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 management console 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 4-1).

Table 4-1 Assigning Privileged-Level Passwords

Privileged-Level Password	Assigned from...
Unencrypted	• [P] Console Password option on the Management Console Logon Screen • [M] Modify password option on the Console Settings Menu • CLI
Encrypted	• 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 "Network Management (SNMP) Configuration Menu" section on page 4-24.

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

Cluster Member Password

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*.

System Configuration Menu

To display the System Configuration Menu (Figure 4-5), enter the **[S] System** option from the Management Console Main Menu.

Figure 4-5 System Configuration Menu

```
Catalyst 1900 - System Configuration
System Revision:  0   Address Capacity:  1024
System UpTime:    0day(s) 00hour(s) 11minute(s) 29second(s)

--------------------Settings------------------
[N] Name of system
[C] Contact name
[L] Location
[S] Switching mode                              FragmentFree
[U] Use of store-and-forward for multicast      Disabled
[A] Action upon address violation               Suspend
[G] Generate alert on address violation         Enabled
[I] Address aging time                          300 second(s)
[P] Network Port                                None
[H] Half duplex back pressure   (10-mbps ports) Disabled
[E] Enhanced Congestion Control (10 Mbps Ports) Disabled

--------------------Actions-------------------
[R] Reset system                    [F] Reset to factory defaults
-----------------Related Menus---------------
[B] Broadcast storm control         [X] Exit to Main Menu

Enter Selection
```

Note If your switch is running the Cisco Catalyst 1900/2820 Enterprise Edition Software, the System Configuration Menu provides the options to enable and disable bridge groups and VLANs. For information about VLANs, see the *Catalyst 1900 Series and Catalyst 2820 Series Enterprise Edition Software Configuration Guide*.

[N] Name of system—Enter the name (up to 255 characters) of the switch. The name you assign to the switch is kept even when the switch joins or leaves a cluster.

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.

[C] Contact name—Enter of the name (up to 255 characters) of the person responsible for managing the switch.

[L] Location—Enter the physical location (up to 255 characters) of the switch.

[S] Switching mode—Set the switching mode to either FragmentFree (cut-through) or store-and-forward. The default is FragmentFree. For additional information, see "Switching Modes" section on page 4-16.

[U] Use of store-and-forward for multicast—Enter [**E]**nable if you want the switch to use store-and-forward mode for multicast packets. Enter [**D]**isable if you want to use the FragmentFree (cut-through) switching mode. 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. The default is [D]isable.

[A] Action upon address violation—Enter one of the following options:

- [**S**]uspend (default)—The port stops forwarding until a packet with a valid source address is received.
- [**D**]isable—The port is disabled until its status is manually re-enabled.
- [**I**]gnore—The port status remains unchanged.

The default action is [S]uspend.

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. For information about secure ports, see the “Port Statistics Report” section on page 4-59.

[G] Generate alert on address violation—Enter [**E**]nable if you want the switch to generate SNMP alerts if an address violation occurs. Enter [**D**]isable to disable this option. This option enables the switch to generate SNMP alerts if an address violation occurs. The default is [E]nable.

Note Traps are sent to the trap managers defined on the Network Management (SNMP) Configuration Menu.

[I] Address aging time—Enter the number of seconds (10 to 1000000; where 1000000 seconds is approximately 11 1/2 days) the switch stores an inactive entry, after which it is removed from the table. The default is 300 seconds (5 minutes). This value applies to all dynamic addresses in the Dynamic Address Table.

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

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

[P] Network Port—Enter the number of the port that you want to designate as the network port. By default, no port is assigned as the network port. The network port is the destination port for all packets with unknown unicast addresses. 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.

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.

For more information about unicast addresses, see the "Port Addressing Menu" section on page 4-53 and the "Flooding of Unknown MAC Addresses" section on page 4-58.

[H] Half duplex back pressure (10-Mbps ports)—Enter [**E**]nable if you want the switch to apply back pressure on all half-duplex 10-Mbps ports. Enter [**D**]isable to disable this option. The default is [D]isable.

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 "Port Configuration Menu" section on page 4-44.

[E] Enhanced Congestion Control (10-Mbps ports)—Enter one of the following options:

- [**1**] 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.
- [**2**] Disabled (Default)—Causes the port to operate under the standard IEEE 802.3 backoff algorithm for retransmitting frames.
- [**3**] Moderately Aggressive—Causes the port to use a modified backoff algorithm to more aggressively retransmit frames and empty the queue.
- [**4**] 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.

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 "Port Configuration Menu" section on page 4-44. ECC on the 100-Mbps ports is set on a per-port basis, not on a global basis.

[R] Reset system—Enter [**Y**]es to reset the switch. All configured system parameters and static addresses are retained; all dynamic addresses are removed.

[F] Reset to factory defaults—Enter [**Y**]es to reset the switch and return it to its factory settings. All static and dynamic addresses are removed, as are the IP address and all other configuration parameters.

Note If the switch is a cluster member, using the [F] Reset to factory defaults option removes the switch from the cluster.

We recommend using the command-switch management interfaces to remove member switches from a cluster. If you want to add the switch to a cluster but had previously used the [F] Reset to factory defaults option to remove it from a cluster, you must use one of the command-switch management interfaces to remove and then add the switch.

[B] Broadcast storm control—Display the Broadcast Storm Control Menu. You can use this menu to inhibit the forwarding of broadcast packets when large numbers or *storms* of broadcast packets are received by a port. For more information, see the "Broadcast Storm Control Menu" section on page 4-17.

[X] Exit—Display the Management Console Main Menu.

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.

Although Table 4-2 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 4-3 shows the minimum and maximum packet reception latencies, which you need to add to the store-and-forward latencies in Table 4-2.

Table 4-2 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 4-3 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

Broadcast Storm Control Menu

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 affected. Broadcast storm control allows you to control the quantity of broadcast packets the switch forwards to your network, thus reserve 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 “Flooding of Unknown MAC Addresses” section on page 4-58 and the “Multicast Registration Menu” section on page 4-66.

To display the Broadcast Storm Control Menu (Figure 4-6), enter the **[B] Broadcast storm control** option from the System Configuration Menu.

Figure 4-6 Broadcast Storm Control Menu

```
Catalyst 1900 - Broadcast Storm Control

--------------------Settings------------------

[A] Action upon exceeding broadcast threshold   Ignore
[G] Generate alert when threshold exceeded      Disabled

[T] Broadcast threshold (BC's received / sec)   500
[R] Broadcast re-enable threshold               250

[X] Exit to previous menu

Enter Selection:
```

[A] Action upon exceeding broadcast threshold—Enter [**B**]lock or [**I**]gnore for the action the switch takes when the broadcast threshold is exceeded. The default is [I]gnore.

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.

[G] Generate alert when threshold exceeded—Enter [**E**]nable if you want the switch to generate SNMP alerts when the broadcast threshold is exceeded. Enter [**D**]isable to disable this option. The alert generated is the trapbroadcastStorm. A trap is generated every 30 seconds. The default is [D]isable.

[T] Broadcast threshold (BCs received/sec)—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.

[R] Broadcast re-enabled threshold—Enter the threshold below which broadcast forwarding is re-enabled. The range is 10 to 14400 packets. The default is 250.

[X] Exit—Display the System Configuration Menu.

Network Management Menu

To display the Network Management Menu (Figure 4-7), enter the **[N] Network Management** option from the Management Console Main Menu.

Figure 4-7 Network Management Menu

```
Catalyst 1900 - Network Management

[I] IP Configuration
[S] SNMP Management
[B] Bridge - Spanning Tree
[C] Cisco Discovery Protocol
[G] Cisco Group Management Protocol
[H] HTTP Server Configuration
[R] Cluster Management

[X] Exit to Main Menu

Enter Selection:
```

[I] IP Configuration—Display the IP Configuration Menu.

[S] SNMP Management—Display the Network Management (SNMP) Configuration Menu.

[B] Bridge–Spanning-Tree—Display the Spanning Tree Configuration Menu.

[C] Cisco Discovery Protocol—Display the CDP Configuration/Status Menu.

[G] Cisco Group Management Protocol—Display the Cisco Group Management Protocol (CGMP) Configuration Menu.

[H] HTTP Server Configuration—Display the HTTP Server Configuration Menu.

[R] Cluster Management—Display the Cluster Management Menu.

[X] Exit—Display the Management Console Main Menu.

IP Configuration Menu

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 display the IP Configuration Menu (Figure 4-8), enter the **[I] IP Configuration** option from the Network Management Menu.

Figure 4-8 IP Configuration Menu

```
Catalyst 1900 - IP Configuration

Ethernet Address:  00-E0-1E-7E-B4-40

--------------------Settings-----------------
[I] IP address                              0.0.0.0
[S] Subnet mask                             0.0.0.0
[G] Default gateway                         0.0.0.0
[B] Management Bridge Group                 1 (fixed)
[M] IP address of DNS server 1              0.0.0.0
[N] IP address of DNS server 2              0.0.0.0
[D] Domain name
[R] Use Routing Information Protocol        Enabled

---------------------- Actions ----------------------------------------
[P] Ping
[C] Clear cached DNS entries
[X] Exit to previous menu

Enter Selection:
```

[I] IP address—Assign an IP address to the switch. 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 assigns it an IP address automatically.

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 menu will end your Telnet session to the switch. You will need to start another Telnet session and use the new IP address of the 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.

[S] Subnet mask—Enter the subnet mask for the switch. Subnet masks exist only if the network has been divided up into subnetworks.

[G] Default gateway—Enter the IP address of the default gateway. Use dotted quad format (nnn.nnn.nnn.nnn). If the switch is connected to a DNS server, you can enter the name of the router instead. 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 assignment of a gateway, see the [R] Use Routing Information Protocol option on the IP Configuration Menu.

[B] Management bridge group—Displays the management bridge group, which is always bridge group 1. The switch IP address must be assigned to a management bridge group to enable the switch to communicate with devices within the bridge group without use of a router. Devices in other bridge groups can only communicate with the switch if the other bridge groups are connected to the management bridge group by a router.

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

[M] IP address of DNS server 1—Enter the IP address of the Domain Name System (DNS) server in the IP Address of DNS Server 1 field. Use dotted quad format (nnn.nnn.nnn.nnn).

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 instead of its IP address from the switch management interfaces, the DNS server associated with the switch looks up the name before forwarding the packet to the destination device. The switch can be associated to up to two DNS servers.

[N] IP address of DNS server 2—Enter the IP address of a second DNS server. Use dotted quad format (nnn.nnn.nnn.nnn).

[D] Domain name—Enter the domain name (up to 62 characters) of the DNS server to which the switch is associated (such as cisco.com).

[R] Use Routing Information Protocol—Enter [**E**]nable if you want the Routing Information Protocol (RIP) to automatically discover and assign an IP gateway to the switch. Enter [**D**]isable to disable this option. The default is [E]nable.

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.

[P] Ping—Enter the IP address of a device that can communicate with switch. Use dotted quad format (nnn.nnn.nnn.nnn). If the switch is connected to a DNS server, you can enter the name of the device instead.

[C] Clear cached DNS entries—Enter [**Y**]es if you want to purge all the cached DNS entries. Enter [**N**]o to display the IP Configuration Menu.

[X] Exit—Display the Network Management Menu.

Network Management (SNMP) Configuration Menu

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 Network Management (SNMP) Configuration Menu (Figure 4-9), enter the **[S] SNMP Management** option from the Network Management Menu.

Figure 4-9 Network Management (SNMP) Configuration Menu

```
Catalyst 1900 - Network Management (SNMP) Configuration

[R] READ configuration
[W] WRITE configuration
[T] TRAP configuration

[X] Exit to previous menu

Enter Selection:
```

[R] READ Configuration—Display the Network Management (SNMP) READ Configuration Menu.

[W] WRITE Configuration—Display the Network Management (SNMP) WRITE Configuration Menu.

[T] TRAP Configuration—Display the Network Management (SNMP) TRAP Configuration Menu.

[X] Exit—Display the Network Management Menu.

Network Management (SNMP) READ Configuration Menu

To display the Network Management (SNMP) READ Configuration Menu (Figure 4-10), enter the **[R] READ configuration** option from the Network Management (SNMP) Configuration Menu.

Figure 4-10 Network Management (SNMP) READ Configuration Menu

```
Catalyst 1900 - Network Management (SNMP) READ Configuration

---------------------- Settings ------------------------------------

[1] First  READ community string
[2] Second READ community string
[3] Third  READ community string
[4] Fourth READ community string

[X] Exit to previous menu

Enter Selection:
```

[1–4] READ community strings—Enter the community string(s) (up to 32 characters). 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.

[X] Exit—Display the Network Management (SNMP) Configuration Menu.

Network Management (SNMP) WRITE Configuration Menu

To display the Network Management (SNMP) WRITE Configuration Menu (Figure 4-11), enter the **[W] WRITE configuration** option from the Network Management (SNMP) Configuration Menu.

Figure 4-11 Network Management (SNMP) WRITE Configuration Menu

```
Catalyst 1900 - Network Management (SNMP) WRITE Configuration

---------------------- Settings ------------------------------------

[1] First  WRITE community string
[2] Second WRITE community string
[3] Third  WRITE community string
[4] Fourth WRITE community string

[A] First  WRITE manager name or IP address
[B] Second WRITE manager name or IP address
[C] Third  WRITE manager name or IP address
[D] Fourth WRITE manager name or IP address

[X] Exit to previous menu

Enter Selection:
```

[1–4] WRITE community strings—Enter the community string(s) (up to 32 characters). 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 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.

[A–D] WRITE manager names or IP addresses—Enter the IP address(es) or name(s) of the SNMP management station(s) that can issue write requests to the switch. Use dotted quad format (nnn.nnn.nnn.nnn). If the switch is connected to a DNS server, you can enter the name of the management station(s) instead. To remove a write manager, press the **Backspace** key to erase characters.

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 Network Management (SNMP) WRITE Configuration Menu or the SNMP Management Page.

[X] Exit—Display the Network Management (SNMP) Configuration Menu.

Network Management (SNMP) TRAP Configuration Menu

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 only use its accompanying community string; 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.

To display the Network Management (SNMP) TRAP Configuration Menu (Figure 4-12), enter the **[T] TRAP configuration** option from the Network Management (SNMP) Configuration Menu.

Figure 4-12 Network Management (SNMP) TRAP Configuration Menu

```
Catalyst 1900 - Network Management (SNMP) TRAP Configuration

---------------------- Settings ------------------------------------

[1] First  TRAP community string
[A] First  TRAP manager name or IP address

[2] Second TRAP community string
[B] Second TRAP manager name or IP address

[3] Third  TRAP community string
[C] Third  TRAP manager name or IP address

[4] Fourth TRAP community string
[D] Fourth TRAP manager name or IP address

[U] Authentication trap generation              Enabled
[L] LinkUp/LinkDown trap generation             Enabled

[X] Exit to previous menu

Enter Selection:
```

Note A trap manager can only use its accompanying community string; it cannot use the community string of another trap manager.

[1–4] TRAP community strings—Enter the community string(s) (up to 32 characters). You can assign up to four community strings to serve as passwords that enable the switch to validate trap requests from a management station.

[A–D] TRAP manager names or IP addresses—Enter the IP address of the SNMP management station(s) that can issue trap requests to the switch. Use dotted quad format (nnn.nnn.nnn.nnn). If the switch is connected to a DNS server, you can enter the name of the management station(s) instead.

To remove a trap manager, press the **Backspace** key to erase characters.

You can assign up to four trap managers and their accompanying community strings.

[U] Authentication trap generation—Enter [**E**]nable if you want the switch to generate authentication traps, which alerts a management station of SNMP requests not accompanied by a valid community string. Enter [**D**]isable to disable this option. The default is [E]nable.

Note Even if this option is enabled, no traps are generated if no trap manager addresses or names are assigned.

[L] LinkUp/LinkDown trap generation—Enter **[E]**nable if you want 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.

Enter [**D**]isable to disable this option. The default is [E]nable.

[X] Exit—Display the Network Management (SNMP) Configuration Menu.

Spanning Tree Configuration Menu

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.

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 Overlapping ports should be connected to end nodes only, not to other bridges. To configure bridge groups, use the Bridge Group Configuration Menu on the management console.

For more information about bridge groups, see the “Bridge Group Configuration Menu” on page 64. 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 display the Spanning Tree Configuration Menu (Figure 4-13), enter the **[B] Bridge - Spanning Tree** option from the Network Management Menu.

Figure 4-13 Spanning Tree Configuration Menu

```
Catalyst 1900 - Bridge Group 1 - Spanning Tree Configuration
Bridge ID: 8000 00-E0-1E-81-1E-40

--------------------Information----------------
Designated root 8000 00-E0-1E-81-1E-40
Number of member ports    27   Root port               N/A
Max age (sec)             20   Root path cost            0
Forward Delay (sec)       15   Hello time (sec)          2
Topology changes           0   Last TopChange   0d00h00m00s

--------------------Settings-----------------
[S] Spanning Tree Algorithm & Protocol          Enabled
[B] Bridge priority                             32768 (8000 hex)
[M] Max age when operating as root              20 second(s)
[H] Hello time when operating as root           2 second(s)
[F] Forward delay when operating as root        15 second(s)

--------------------Actions------------------
[N] Next bridge group         [G] Goto bridge group
[P] Previous bridge group     [X] Exit to previous menu

Enter Selection:
```

Spanning-Tree Root Settings

The Information fields on this menu display 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.

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.

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

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. See the "Port Configuration Menu" section on page 4-44 for Port Fast mode configuration instructions.

[S] Spanning-Tree Algorithm and Protocol—Enter [**E**]nable or [**D**]isable the Spanning-Tree Protocol (STP) to ensure a loop-free configuration in the bridge topology. When STP is enabled, redundant ports are kept in standby (suspended) status and are enabled when needed. The default is [E]nable.

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.

[B] Bridge priority—Enter a 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.

[M] Max age when operating as root—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.

[H] Hello time when operating as root—Enter the number of seconds (1 to 10) between the transmission of STP configuration messages. The default is 2.

[F] Forward delay when operating as root—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.

[N] Next bridge group—Display the Spanning-Tree configuration for the next sequentially numbered bridge group.

[G] Goto bridge group—Display the Spanning-Tree configuration for a specified bridge group.

[P] Previous bridge group—Display the Spanning-Tree configuration for the previous sequentially numbered bridge group.

[X] Exit—Display the Network Management Menu.

CDP Configuration/Status Menu

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 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 Configuration/Status Menu (Figure 4-14), enter the **[C] Cisco Discovery Protocol** option from the Network Management Menu.

Figure 4-14 CDP Configuration/Status Menu

```
Catalyst 1900 - CDP Configuration/Status

CDP enabled on: 1-24, AUI, A, B

--------------------Settings------------------

[V] Version                                    2
[H] Hold Time (secs)                         180
[T] Transmission Interval (secs)              60

--------------------Actions-------------------

[E] Enable CDP on Port(s)
[D] Disable CDP on Port(s)
[S] Show Neighbor
[X] Exit to previous menu

Enter Selection:
```

[V] Version—Enter the version [**1]** or [**2]** the switch uses. Version 1 provides standard CDP support. Version 2 is required for the switch to be a cluster member. When the switch is using version 2, it can still interoperate with neighboring Cisco devices running version 1. The default is 2.

Note We recommend using version 2, which must be enabled before the switch joins a cluster.

[H] Hold Time—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.

[T] Transmission Interval— 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.

[E] Enable CDP on Port(s)—Enter the port(s) that you want to exchange information with Cisco devices. The defaults for all ports is [E]nable.

Enter the port numbers according to these conventions:

- Separate the port numbers with a hyphen to create a range, or use commas or spaces between port numbers.
- Enter **A** or **B** to run CDP on the 100-Mbps ports.
- Enter **ALL** to assign all the switch ports. The defaults for all ports is [E]nable.

[D] Disable CDP on Port(s)—Enter the ports on which you want to disable CDP. Use the conventions described in the previous paragraph.

[S] Show Neighbor—Display the following information about that device (see also Figure 4-15). The first two lines in the display define the abbreviations used.

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 IP Address column.

Figure 4-15 Show Neighbor Display

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, P - Repeater, H - Host, I - IGMP
DeviceID      IP Addr     Local Port  Capability  Platform   Remote Port
00E01E871FC0 10.1.126.46     4         TS       cisco 1900    3
00C01D80727  10.1.126.47     6         TS       cisco 1900    10

Press any key to continue.
```

[X] Exit—Display the Network Management Menu.

Cisco Group Management Protocol Configuration Menu

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 additional information, see the

- "Flooding of Unknown MAC Addresses" section on page 4-58
- "Port Statistics Report" section on page 4-59,
- "Multicast Registration Menu" section on page 4-66

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

To display the Cisco Group Management Protocol (CGMP) Configuration Menu (Figure 4-16), enter the **[G] Cisco Group Management Protocol** option from the Network Management Menu.

Figure 4-16 Cisco Group Management Protocol (CGMP) Configuration Menu

```
Catalyst 1900 - Cisco Group Management Protocol (CGMP) Configuration

--------------------Settings------------------

[H] Router Hold Time (secs)               600
[C] CGMP                                  Enabled
[F] CGMP Fast Leave                       Disabled

--------------------Actions-------------------
[L] List IP multicast addresses
[R] Remove IP multicast addresses

[X] Exit to previous menu

Enter Selection:
```

[H] Router Hold Time (secs)—Enter the number of seconds (between 5 and 900) 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.

[C] CGMP—Enter [**E**]nable to enable CGMP on the switch. Enter [**D**]isable this option. The default is [E]nable.

[F] CGMP Fast Leave—Enter [**E**]nable to enable CGMP Fast Leave on the switch. Enter [**D**]isable this option. The default is [D]isable.

The Fast Leave option can eliminate unnecessary multicast traffic to switch ports, which no longer have group members interested in that specific multicast traffic.

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.

[L] List IP multicast addresses—Display a list, which the switch automatically creates and dynamically maintains, of the addresses of designated multicast recipients and the associated switch port(s) through which multicast traffic are forwarded to those recipients. This list is also known as the IP Multicast Address Table.

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.

[R] Remove IP multicast addresses—Remove an IP multicast address from the IP multicast address list.

Caution Use the [R] Remove IP multicast addresses option only to debug and recover from unexpected situations.

[X] Exit—Display the Network Management Menu.

HTTP Server Configuration Menu

To display the HTTP Server Configuration Menu (Figure 4-17), enter the **[H] HTTP Server Configuration** option from the Network Management Menu.

Figure 4-17 HTTP Server Configuration Menu

```
Catalyst 1900 - HTTP Server Configuration

---------------------- Settings -------------------------------------

[H] HTTP                                    Enabled
[P] HTTP Port                               80

[X] Exit to previous menu

Enter Selection:
```

[H] HTTP—Enter [**E**]nable if you want to access the Catalyst 1900 Switch Manager through one of the switch ports. Enter [**D**]isable to disable this option. The default is [E]nable.

Note 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. Changes to the switch IP information should be done with care.

[P] HTTP Port—Enter a port number (0 to 65535) on which the HTTP server listens for HTTP connections. The default is 80.

[X] Exit—Display the Network Management Menu.

Cluster Management Menu

You can configure and monitor the switch from a Catalyst 2900 XL or Catalyst 3500 XL command switch if the switch is member of a switch cluster. All cluster management tasks (such as joining a cluster) are performed from the Cluster Management applications on the command switch. However, you can use this menu to remove the switch from the cluster.

For the requirements on becoming a cluster member and the configuration changes upon joining a cluster, see the "Cluster Management and Membership" section on page 1-17. For complete 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 Cluster Management Menu (Figure 4-18), enter the **[R] Cluster Management** option from the Network Management Menu.

Figure 4-18 Cluster Management Menu

```
Catalyst 1900 - Cluster Management

---------------------- Information -----------------------------------
Cluster name
Member number
Management IP address                      0.0.0.0
Command device MAC address

---------------------- Actions ---------------------------------------
[R] Remove From Cluster

[X] Exit to Main Menu

Enter Selection:
```

When the switch is a cluster member, the display fields on this menu show the cluster name (which is not the same as the command switch name), IP address, and MAC address of the command switch. This menu also displays the membership number of the switch as a member switch.

[R] Remove From Cluster—Remove the switch from its current cluster.

Note If the switch is a cluster member, using the [R] Remove From Cluster option removes the switch from the cluster.

We recommend using the command-switch management interfaces to remove member switches from a cluster. If you want to add the switch to a cluster but had previously used the [R] Remove From Cluster option to remove it from a cluster, you must use one of the command-switch management interfaces to remove and then add the switch.

[X] Exit—Display the Network Management Menu.

Port Configuration Menu

When you enter the **[P] Port Configuration** option from the Management Console Main Menu, the following prompt is displayed:

```
Identify Port:  1 to 24[1-24], [AUI], [A], [B]:
Select [1 - 24, AUI, A, B]:
```

At the prompt, enter the specific port that you want to configure.

- If you select a 10BaseT port (ports 1x through 12x or 24x or AUI), the Port Configuration Menu (10BaseT Ports) in Figure 4-19 is displayed.
- If you select a 100BaseT port (ports Ax or Bx), the Port Configuration Menu (100BaseT Ports) in Figure 4-20 is displayed.

Figure 4-19 Port Configuration Menu (10BaseT Ports)

```
Catalyst 1900 - Port 1 Configuration

Built-in 10Base-T
802.1d STP State:  Blocking     Forward Transitions:  0

--------------------Settings------------------
[D] Description/name of port
[S] Status of port                              Suspended-no-linkbeat
[F] Full duplex                                 Disabled
[I] Port priority (spanning tree)               128 (80 hex)
[C] Path cost (spanning tree)                   100
[H] Port fast mode (spanning tree)              Enabled

------------------Related Menus---------------
[A] Port addressing           [V] View port statistics
[N] Next port                 [G] Goto port
[P] Previous port             [X] Exit to Main Menu

Enter Selection:
```

Figure 4-20 Port Configuration Menu (100BaseT Ports)

```
Catalyst 1900 - Port A Configuration

Built-in:  100Base-TX
802.1d STP State:  Blocking     Forward Transitions:  0

---------------------- Settings ------------------------------------
[D] Description/name of port
[S] Status of port
[I] Port priority (spanning tree)              128 (80 hex)
[C] Path cost (spanning tree)                  10
[H] Port fast mode (spanning tree)             Disabled
[E] Enhanced congestion control                Disabled
[F] Full duplex / Flow control                 Half duplex

---------------------- Related Menus -------------------------------
[A] Port addressing          [V] View port statistics
[N] Next port                [G] Goto port
[P] Previous port            [X] Exit to Main Menu

Enter Selection:
```

Note Figure 4-20 displays the menu for configuring the 100BaseTX ports. The port configuration menus for the 100BaseFX and 100-Mbps fiber-optic ports are similar.

The STP State field displays the STP 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.

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.

[D] Description/name of port—Enter the name or description (up to 60 characters) of the port.

[S] Status of port—Enter [**E**]nable to enable the port to transmit and receive data. Enter **[D**]isable to disable the port. The default is [E]nable.

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 4-4.

Table 4-4 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.

[F] Full duplex (10-Mbps ports)—Enter [**E**] to enable full-duplex transmission on a 10BaseT port. Enter [**D**]isable if you want the ports to operate in half duplex. The default is [D]isable (half duplex enabled).

For more information about the duplex mode, see the "Full-Duplex Operation" section on page 4-52. For information about using the half-duplex back pressure option on the 10-Mbps ports, see the "System Configuration Menu" section on page 4-11.

[F] Full-duplex/Flow Control (100-Mbps ports)—Enter one of the settings: [**1**] Full duplex, [**2**] Half duplex, [**3**] Full duplex with flow control, or [**4**] Autonegotiate. The default of the 100BaseTX ports is [4] Autonegotiate. The default of the 100-Mbps fiber-optic ports is [2] Half duplex.

Note Flow control on full-duplex ports is available only on the 100-Mbps ports. Duplex autonegotiation is available only on the 100BaseTX ports, not on the 10BaseT ports or the 100-Mbps fiber-optic ports.

For more information about this option, see the

- "Full-Duplex Operation" section on page 4-52
- "Flow Control" section on page 4-52
- "Autonegotiation" section on page 4-52

[I] Port priority—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.

[C] Path cost—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.

[H] Port Fast mode—Enter [**E**]nable to enable Port Fast on a port. The default for the 10-Mbps ports is [E]nable. The default for the 100-Mbps ports is [D]isable.

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.

[E] Enhanced congestion control (100-Mbps ports)—Enter one of the following options:

- [**1**] 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.
- [**2**] Disabled (Default)—Causes the port to operate under the standard IEEE 802.3 backoff algorithm for retransmitting frames.
- [**3**] Moderately Aggressive—Causes the port to use a modified backoff algorithm to more aggressively retransmit frames and empty the queue.
- [**4**] 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.

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 per-port basis on the 100-Mbps ports.

For information about ECC on the 10-Mbps ports, see the System Configuration Menu. ECC on the 10-Mbps ports is set on a global basis, not on a per-port basis.

[A] Port addressing—Display the Port Addressing Menu.

[V] View port statistics—Display the Detailed Port Statistics Report.

[N] Next port—Display the Port Configuration Menu for the next sequentially numbered port of the switch.

[G] Go to port—Display the Port Configuration Menu for a specified port. The following prompt is displayed:

```
Identify Port:  1 to 24[1-24], [AUI], [A], [B]:
Select [1 - 24, AUI, A, B]:
```

[P] Previous port—Display the Port Configuration Menu for the port number that is one less than the current port. (That is, if you are viewing the menu for port 5 and you select this option, the menu for port 4 is displayed.)

[X] Exit—Display the Management Console Main Menu.

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 "System Configuration Menu" section on page 4-11.

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.

Port Addressing Menu

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:

- "Flooding of Unknown MAC Addresses" section on page 4-58
- "System Configuration Menu" section on page 4-11
- "Broadcast Storm Control Menu" section on page 4-17
- "Cisco Group Management Protocol Configuration Menu" section on page 4-39
- "Multicast Registration Menu" section on page 4-66

When you enter the **[A] Port Addressing** option from the Management Console Main Menu, the following prompt is displayed:

```
Identify Port:  1 to 24[1-24], [AUI], [A], [B]:
Select [1 - 24, AUI, A, B]:
```

At the prompt, enter the specific port that you want to configure. The Port Addressing Menu (Figure 4-21) is displayed.

Figure 4-21 Port Addressing Menu

```
Catalyst 1900 - Port 1 Addressing

Address  : Unaddressed

---------------------- Settings ----------------------------------------
[T] Address table size                          Unrestricted
[S] Addressing security                         Disabled
[K] Clear addresses on link down                Disabled
[U] Flood unknown unicasts                      Enabled
[M] Flood unregistered multicasts               Enabled

---------------------- Actions -----------------------------------------
[A] Add a static address
[D] Define restricted static address
[L] List addresses
[E] Erase an address
[R] Remove all addresses

[C] Configure port            [V] View port statistics
[N] Next port                 [G] Goto port
[P] Previous port             [X] Exit to Main Menu

Enter Selection:
```

The top of the menu displays the current addressing situation:

- Dynamic addresses—The current number of unicast addresses that have been automatically learned on this port. If this is a secured port, the dynamic addresses field is set to 0.

  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.

- Static addresses—The current number of unicast addresses that have been assigned to this port.

  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 assigned (static) or *sticky-learned* (see the [D] Define a restricted static address option on this menu). If the address table is full, an error message is generated. You can change the size of the address table by using the [T] Address Table Size option on this menu.

[T] Address Table Size—Enter the number (1 and 132) of addresses assigned to a secure port. If the port is not a secure port, 0 is the value in Address Table Size field. 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.

[S] Addressing security—Enter [**E**]nable to secure the port. Enter [**D**]isable to disable this option. The default is [D]isable.

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. For information about static addresses, see the [D] Define a restricted static address option on this menu.

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 information about the network port, see the “System Configuration Menu” section on page 4-11.

[K] Clear addresses on link down—Enter [**E**]nable if you want the port to clear its address associations on linkDown. Enter [**D**]isable if you want the port to retain its association with all static addresses even if it loses link. The default is [D]isable.

Note This option is applicable only when the [S] Addressing security option is enabled on the port.

[U] Flood unknown unicasts—Enter [**E**]nable if you want unknown unicast addresses forwarded to the port. Enter [**D**]isable to prevent forwarding of unknown unicast addresses to this port. The default is [E]nable. For more information, see the "Flooding of Unknown MAC Addresses" section on page 4-58.

You can assign a network port to which all unknown unicast addresses are forwarded. For more information, see the "System Configuration Menu" section on page 4-11.

[M] Flood unregistered multicasts—Enter [**E**]nable if you want unknown unregistered multicast addresses forwarded to this port. Enter [**D**]isable to prevent forwarding of unknown multicast addresses to this port. The default is [E]nable. For more information, see the "Flooding of Unknown MAC Addresses" section on page 4-58.

[A] Add a static address—Enter the unicast source MAC address. Use six hexadecimal octets, spaces are optional (such as hh hh hh hh hh hh or hhhhhhhhhhhh).

Note Only unicast addresses can be added. An attempt to add a multicast or broadcast address will not be accepted and will generate an error message.

Static entries do not age out and must be manually removed from the table.

[D] Define a restricted static address—Enter the unicast or multicast source MAC address in this field. Use six hexadecimal octets, spaces are optional (such as hh hh hh hh hh hh or hhhhhhhhhhhh). You are then prompted to enter the port numbers allowed to send to this address. If there are any typing errors, the prompt is redisplayed.

A restricted static address is accompanied by a list of ports that are allowed to send packets to this address and port.

[L] List addresses—List all dynamic and static addresses that belong to this port. The switch displays up to 15 addresses per display; static addresses are listed first.

[E] Erase an address—Remove a dynamic or static address assigned to the current port. Static entries do not age out and must be manually removed from the address table.

[R] Remove all addresses—Enter [**Y**]es to remove all dynamic and static addresses currently associated with the port. Enter [**N**]o to retain the address associations on the port. Static entries do not age out and must be manually removed from the address table.

[C] Configure port—Display the Port Configuration Menu.

[V] View port statistics—Display the Detailed Port Statistics Report.

[N] Next port—Display the Port Addressing Menu for the next sequentially numbered port of the switch.

[G] Go to port—Display the Port Addressing Menu for a specified port. The following prompt is displayed:

```
Identify Port:  1 to 24[1-24], [AUI], [A], [B]:
Select [1 - 24, AUI, A, B]:
```

[P] Previous port—Display the Port Addressing Menu for the port number that is one less than the current port. (That is, if you are viewing the menu for port 5 and you select this option, the menu for port 4 is displayed.)

[X] Exit—Display the Management Console Main Menu.

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 “System Configuration Menu” section on page 4-11.

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

For information about multicast packet control, see the “Cisco Group Management Protocol Configuration Menu” section on page 4-39. For information about broadcast storm control, see the “Broadcast Storm Control Menu” section on page 4-17.

Port Statistics Report

The Detailed Port Statistics Report 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 menu. 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

Note If you are using VT100 terminal emulation, the statistics on this menu are refreshed every 5 seconds. If you are connected to the management console through a modem running at less than 2400 baud, the statistics displays are refreshed every 8 seconds. Press **Return** or the **Spacebar** to refresh these reports at any time.

When you enter the **[D] Port Statistics Detail** option from the Management Console Main Menu, the following prompt is displayed:

```
Identify Port:  1 to 24[1-24], [AUI], [A], [B]:
Select [1 - 24, AUI, A, B]:
```

At the prompt, enter the specific port for which you want to display the statistics and errors. The Detailed Port Statistics Report (Figure 4-22) is displayed. The errors are described in Table 4-5.

Figure 4-22 is an example statistics report for a 10BaseT port. It is similar to the report for the 100BaseT ports.

Figure 4-22 Detailed Port Statistics Report

```
Catalyst 1900 - Port 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

Select [A] Port addressing, [C] Configure port,
       [N] Next port, [P] Previous port, [G] Goto port,
       [R] Reset port statistics, or [X] Exit to Main Menu:
```

Table 4-5 Error Descriptions

Heading 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 check.
Giant frames	Number of frames received on a particular interface that exceed the maximum permitted frame size.
Address violations	Number of times a source address was seen on this secured port 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 that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.
Excessive deferrals	Number of frames for which transmission is deferred 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.

[A] Port addressing—Display the Port Addressing Menu.

[C] Configure port—Display the Port Configuration Menu.

[R] Reset port statistics—Enter [**Y**]es to clear the port statistics. To update the display, press the **Spacebar.**

[N] Next port—Display the Detailed Port Statistics Report for the next sequentially numbered port of the switch.

[G] Go to port—Display the Detailed Port Statistics Report for a specified port. The following prompt is displayed:

```
Identify Port:  1 to 24[1-24], [AUI], [A], [B]:
Select [1 - 24, AUI, A, B]:
```

[P] Previous port—Display the Detailed Port Statistics Report for the port number that is one less than the current port. (That is, if you are viewing the menu for port 5 and you select this option, the menu for port 4 is displayed.)

[X] Exit—Display the Management Console Main Menu.

Monitoring Configuration Menu

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 Monitoring Configuration Menu (Figure 4-23), enter the **[M] Monitoring** option from the Management Console Main Menu.

Figure 4-23 Monitoring Configuration Menu

```
Catalyst 1900 - Monitoring Configuration

--------------------Settings------------------
[C] Capturing frames to the Monitor             Disabled
[M] Monitor port assignment                     None
Current capture list:  No ports in list

--------------------Actions-------------------
[A] Add ports to capture list
[D] Delete ports from capture list

[X] Exit to Main Menu

Enter Selection:
```

Note Frame capturing cannot take place until the [C] Capturing frames to the Monitor, [M] Monitor port assignment, and [A] Add ports to capture list options are set.

[C] Capturing frames to the Monitor—Enter [**E**]nable to enable port monitoring on the switch. Enter [**D**]isable to disable port monitoring. The default is [D]isable.

[M] Monitor port assignment—Enter the monitoring port (the port to which captured frames are sent). The default is None.

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.

[A] Add ports to capture list—Enter the port(s) you want to monitor. The port capture list can include any number of the ports, from none to all ports.

[D] Delete ports from capture list—Enter the port(s) you want to delete from the capture list.

[X] Exit—Display the Management Console Main Menu.

Bridge Group Configuration Menu

Bridge groups can create segmented switching domains when you assign switch ports to specific user groups (such as engineering and finance). Traffic is confined to hosts within each bridge group, but not between the bridge groups. Using bridge groups has the following benefits:

- The switch forwards traffic only among the hosts that make up the bridge group, thereby restricting broadcast and multicast traffic (flooding) to only those hosts.
- Bridge groups relieve network congestion and provide additional network security by segmenting traffic to certain areas of the network.

The bridge group option assigns the switch ports to a particular spanning-tree group. Use this menu to organize the ports on the switch into one or more bridge groups. Bridge group 1 is always the management bridge group.

By default, all ports are assigned to bridge group 1. A port must always be a member of at least one bridge group and can belong to more than one bridge group if you enable the [O] Overlapping of Bridge Groups Permitted option.

The switch IP address must be assigned to the management bridge group to allow the switch to communicate with devices within the bridge group without the use of a router. Devices in other bridge groups can only communicate with the switch if the other bridge groups are connected to the management bridge group by a router.

A separate spanning-tree instance runs on each bridge group, and each bridge group participates in a separate spanning tree. Overlapping ports (ports that belong to more than one bridge group) participate in all spanning trees to which they belong.

Note Overlapping ports should be connected to end nodes only, not to other bridges.

Note If the network port is configured, it serves only within the bridge groups of which it is a member.

For information about VLANs, see the *Catalyst 1900 Series and Catalyst 2820 Series Enterprise Edition Software Configuration Guide*.

To display the Bridge Group Configuration Menu (Figure 4-24), enter the **[B] Bridge Group** option from the Management Console Main Menu.

Figure 4-24 Bridge Group Configuration Menu

```
Catalyst 1900 - Bridge Group Configuration

Bridge Group  Member Ports
------------------------------------------------------------------------
1             1-24, AUI, A, B
2             None
3             None
4             None

---------------------- Settings ----------------------------------------
[O] Overlapping of Bridge Groups Permitted      Disabled

---------------------- Actions -----------------------------------------
[M] Move member ports
[X] Exit to Main Menu

Enter Selection:
```

[O] Overlapping of Bridge Groups Permitted—Enter [**E**]nable if you want the ports to belong to more than one bridge group. Enter [**D**]isable to disable this option. The default is [D]isable.

Note This option cannot be disabled if any port belongs to multiple bridge groups.

[M] Move member ports—Remove one or more ports from their current bridge groups and add to another bridge group. This option is available only when the [O] Overlapping of Bridge Groups Permitted option is disabled.

[A] Add member ports—Add one or more ports to a bridge group. The ports are not removed from any bridge groups to which they currently belong. This option is available only when the [O] Overlapping of Bridge Groups Permitted option is enabled.

[D] Delete member ports—Delete one or more ports from a bridge group. The ports are removed *only* if they belong to at least one other bridge group. This option is available only when the [O] Overlapping of Bridge Groups Permitted option is enabled.

[X] Exit—Display the Management Console Main Menu.

Multicast Registration Menu

By default, all multicast packets are forwarded to all ports on the switch. To reduce the amount of multicast flooding on the switch, you can register multicast addresses and list the ports to which these packets are to be forwarded. Unlike dynamic addresses, these Permanent Multicast Address Table entries are manually entered and thus are static. Static entries do not age out and must be manually removed from the table. Besides reducing unnecessary traffic, the multicast registration options open up the possibility of using multicast packets for dedicated groupcast applications such as broadcast video.

You can also disable the normal flooding of unregistered multicast packets on a per-port basis. For information about flooding multicast packets, see the “Flooding of Unknown MAC Addresses” section on page 4-58. For more information about controlling multicast traffic, see the “Cisco Group Management Protocol Configuration Menu” section on page 4-39.

To display the Multicast Registration Menu (Figure 4-25), enter the **[R] Multicast Registration** option from the Management Console Main Menu.

Figure 4-25 Multicast Registration Menu

```
Catalyst 1900 - Multicast Registration

Registered multicast addresses:  0

--------------------Actions-------------------
[R] Register a multicast address
[L] List all multicast addresses
[U] Unregister a multicast address
[E] Erase all multicast addresses

[X] Exit to Main Menu

Enter Selection:
```

The first line of the menu displays the number of registered multicast addresses.

[R] Register a multicast address—Enter the multicast addresses and the ports assigned to forward packets from those addresses. Use six hexadecimal octets, spaces are optional (such as hh hh hh hh hh hh or hhhhhhhhhhhh).

If you enter an invalid multicast address, the prompt refreshes itself so that you can try again. Invalid addresses include nonmulticast addresses, the broadcast address, and reserved multicast addresses, such as those used for Spanning-Tree Protocol.

The switch supports up to 64 IP multicast group registrations.

[L] List all registered multicast addresses—List all registered multicast addresses that exist in the switch. Addresses are listed with the port or ports to which they are assigned. Addresses with an asterisk are subject to source-port filtering.

The entries in the Permanent Multicast Address Table allow multicast addresses to be permanently associated with a switch port. Like the Permanent Unicast Address Table, the entries in the Permanent Multicast Address Table are manually entered.

For more information about source-port filtering, see the “Flooding of Unknown MAC Addresses” section on page 4-58.

[U] Unregister a multicast address—Delete registered multicast addresses. You cannot delete those multicast addresses that are not considered registered.

[E] Erase all registered multicast addresses—Remove all registered multicast addresses.

[X] Exit—Display the Management Console Main Menu.

Firmware Configuration Menu

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. Do not turn off the switch until after the switch resets and begins using the new firmware.

This section also provides information for upgrading the switch firmware:

- "Downloading the Switch Firmware from a TFTP Server" section on page 4-71
- "Downloading the Switch Firmware from a TFTP Client" section on page 4-72
- "Downloading the Switch Firmware with the XMODEM Protocol" section on page 4-73

To display the Firmware Configuration Menu (Figure 4-26), enter the **[F] Firmware** option from the Management Console Main Menu.

Figure 4-26 Firmware Configuration Menu

```
Catalyst 1900 - Firmware Configuration

-----------------System Information------------
FLASH:  1024K bytes
V9.00.00 Standard Edition
Upgrade status:
No upgrade currently in progress.

--------------------Settings------------------
[S] TFTP Server name or IP address
[F] Filename for firmware upgrades
[A] Accept upgrade transfer from other hosts    Disabled

--------------------Actions-------------------
[U] System XMODEM upgrade        [D] Download test subsystem (XMODEM)
[T] System TFTP upgrade          [X] Exit to Main Menu

Enter Selection:
```

The switch firmware version and the size of the Flash memory are displayed in the System Information area in the menu. The Upgrade status field in the System Information area shows if a firmware upgrade is in progress.

[S] TFTP Server name or IP address—Enter the IP address of the TFTP server where the upgrade file is located. Use dotted quad format (nnn.nnn.nnn.nnn). If the switch is connected to a DNS server, you can enter the name of the device instead.

[F] Filename for firmware upgrades—Enter the name of the firmware upgrade file to be downloaded, and press **Return.**

[A] Accept upgrade transfer from other hosts—Enter [**E**]nable if you want the switch to accept an upgrade from another host on the network. Enter [**D**]isable to disable this option. The default is [D]isable.

Note To prevent unauthorized upgrades, disable this option after you upgrade the firmware.

[U] System XMODEM upgrade—Enter [**Y**]es to begin the upgrade using XMODEM protocol. The following prompt appears:

```
Please initiate XMODEM transfer.
Awaiting transfer . . . C
```

C is the first XMODEM/CR protocol request. Use the appropriate application-specific command to start the download. When the download is complete, the switch resets, and the newly downloaded firmware begins to execute. The Management Console Logon Screen is displayed.

Enter [**N**]o to return to the Firmware Configuration Menu.

This option is not available during a Telnet session.

[T] System TFTP upgrade—Begin the upgrade from a TFTP server. The address of the server and the name of the file must already be set.

[D] Download test subsystem (XMODEM)—For Cisco personnel only. This option is not available during a Telnet session.

[X] Exit to Main Menu—Display the Management Console Main Menu.

Downloading the 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 From the Firmware Configuration Menu, enter the **[S] TFTP Server name or IP address** option, and enter the IP address of the TFTP server where the upgrade file is located. Use dotted quad format (nnn.nnn.nnn.nnn).

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

Step 3 Enter the **[F] Filename for firmware upgrades** option from the menu**,** and enter the name of the upgrade file.

Step 4 Enter the **[T] System TFTP upgrade** option from the menu to initiate the TFTP download.

The switch contacts the server to download the upgrade file to the switch.

Step 5 Verify the upgrade is in progress by checking the Upgrade status field in the System Information area on the menu. If the upgrade is in progress, the field reads `in-progress`.

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. 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.

Downloading the 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 Enter the **[A] Accept upgrade transfer from other hosts** option from the menu, and enable this option.

Note To prevent unauthorized upgrades, disable this option after you upgrade the firmware.

Step 4 Use the appropriate command (such as, **put** *upgrade_filename*) to download the upgrade file from the client workstation to the switch.

Step 5 Verify the upgrade is in progress by checking the System Information section of the Firmware Configuration Menu. If the upgrade is in progress, the field reads `in-progress`.

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. 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 Disable the **[A] Accept upgrade transfer from other hosts** option.

Downloading the Switch Firmware with the XMODEM Protocol

This procedure is largely dependent on the modem software you are using. ProComm, HyperTerminal, tip, or minicom are examples of applications that use the XMODEM protocol.

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 by using XMODEM.

Step 1 Download the upgrade file from CCO into an appropriate directory on your XMODEM host.

Step 2 Enter the baud rate (2400, 9600, 19200, 38400, or 57600) of the console port on the switch and the management station. You can set the baud rate for the console port from the RS-232 Port Configuration Menu.

Step 3 From the Firmware Configuration Menu, enter the **[U] System XMODEM upgrade** option to use the XMODEM protocol to download the upgrade file.

Step 4 At the prompt, enter [**Y**]es to start the download.

Step 5 Verify the upgrade is in progress by checking the Upgrade status field in the System Information area on the menu. If the upgrade is in progress, the field reads `in-progress`.

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. 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.

RS-232 Interface Configuration Menu

To display the RS-232 Port Configuration Menu (Figure 4-27), enter the **[I] RS-232 Interface** option from the Management Console Main Menu.

Figure 4-27 RS-232 Port Configuration Menu

```
Catalyst 1900 - RS-232 Interface Configuration

------------------Group Settings--------------
[B] Baud rate                                  9600 baud
[D] Data bits                                  8 bit(s)
[S] Stop bits                                  1 bit(s)
[P] Parity setting                             None

--------------------Settings------------------
[M] Match remote baud rate (auto baud)         Enabled
[A] Auto answer                                Enabled
[N] Number for dial-out connection
[T] Time delay between dial attempts           300
[I] Initialization string for modem

--------------------Actions-------------------
[C] Cancel and restore previous group settings
[G] Activate group settings

[X] Exit to Main Menu

Enter Selection:
```

Note If you change the settings for baud rate, data bits, stops bits, or parity, you must also use the [G] Activate group settings option to activate any of these values or settings.

[B] Baud rate—Enter the baud rate (2400, 9600, 19200, 38400, or 57600) of the console port. The default is 9600.

[D] Data bits—Enter the data bits (7 and 8) for the console port. The default is 8.

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

[S] Stop bits—Enter the stop bits value for the console port. The default is 1.

[P] Parity settings—Change the parity settings for the console port. The default is None.

[M] Match remote baud rate (auto baud)—Enter [**E**]nable to enable the console port to automatically match the baud rate of an incoming call. The switch only matches a baud rate lower than its configured baud rate. After the call, the switch reverts to its configured rate. Enter [**D**]isable to disable this option. The default is [E]nable.

[A] Auto answer—Enter [**E**]nable to enable the switch to automatically answer calls. Enter [**D**]isable to disable this option. The default is [E]nable.

[N] Number for dial-out connection—Enter the phone number (up to 48 characters) the switch is configured to use when dialing out. This number is dialed when the switch is configured to communicate with a remote terminal upon power-up or reset. If the dial-out is unsuccessful and auto-answer is enabled, the switch ceases dialing and awaits incoming calls.

To delete the number, press the **Backspace** key followed by **Return**. Use the format required by your modem when you enter the number.

[T] Time delay between attempts—Enter the number of seconds between dial-out attempts. Zero (0) disables retry. The default is 300 seconds.

[I] Initialization string for modem—Change the initialization string to match your modem requirements. Enter up to 48 characters.

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

[C] Cancel and restore previous group settings—Undo any new values entered for the baud rate, data bits, stop bits, and parity setting. Values are restored to those last saved.

[G] Activate group settings—Activate the settings you have entered for baud rate, data bits, stops bits, and parity. After selecting this option, configure the attached management station to match the new settings.

Note The changes you make to parameters under the heading Group Settings are not invoked until you use the [G] Activate group settings option. Use the [C] Cancel and restore previous group settings option to cancel the session and to return to the previous settings.

[X] Exit—Display the Management Console Main Menu.

Usage Summary Menu

To display the Usage Summary Menu (Figure 4-28), enter the **[U] Usage Summaries** option from the Management Console Main Menu. Use this menu to display summaries of network statistics for all ports. These reports are read-only.

Note If you are using VT100 terminal emulation, the statistics on this menu are refreshed every 5 seconds. If you are connected to the management console via a modem running at less than 2400 baud, the statistics displays are refreshed every 8 seconds. Press **Return** or the **Spacebar** to refresh these reports at any time.

Figure 4-28 Usage Summary Menu

```
Catalyst 1900 - Usage Summaries

[P] Port Status Report
[A] Port Addressing Report
[E] Exception Statistics Report
[U] Utilization Statistics Report
[B] Bandwidth Usage Report

[X] Exit to Main Menu

Enter Selection:
```

[P] Port Status Report—Display the Port Status Report.

[A] Port Addressing Report—Display the Port Addressing Report.

[E] Exception Statistics Report—Display the Exception Statistics Report.

[U] Utilization Statistics Report—Display the Utilization Statistics Report.

[B] Bandwidth Usage Report—Display the Bandwidth Usage Report.

[X] Exit—Display the Management Console Main Menu.

Port Status Report

To display the Port Status Report (Figure 4-29), enter the **[P] Port Status Report** option from the Usage Summary Menu. This report displays a summary of the status of all ports as defined on the Port Configuration Menu. Definitions of these terms can be found in the "Port Configuration Menu" section on page 4-44.

Figure 4-29 Port Status Report

```
Catalyst 1900 - Port Status Report

1  : Suspended-no-linkbeat            13 : Suspended-no-linkbeat
2  : Suspended-no-linkbeat            14 : Enabled
3  : Suspended-no-linkbeat            15 : Enabled
4  : Enabled                          16 : Enabled
5  : Enabled                          17 : Enabled
6  : Enabled                          18 : Enabled
7  : Enabled                          19 : Suspended-no-linkbeat
8  : Suspended-no-linkbeat            20 : Suspended-no-linkbeat
9  : Enabled                          21 : Enabled
10 : Enabled                          22 : Enabled
11 : Enabled                          23 : Suspended-no-linkbeat
12 : Enabled                          24 : Suspended-no-linkbeat
                                      AUI: Enabled
A  : Enabled
B  : Enabled

Monitor port: None; Network port: None

Select [X] Exit to previous menu:
```

[X] Exit—Display the Usage Summary Menu.

Port Addressing Report

To display the Port Addressing Report (Figure 4-30), enter the **[A] Port Addressing Report** option from the Usage Summary Menu. This report displays the address mode (dynamic or static) of each port and how many addresses have been assigned to each port.

Figure 4-30 Port Addressing Report

```
Catalyst 1900 - Port Addressing Report

1  :              Unaddressed          13 :              Unaddressed
2  :              Unaddressed          14 :              Unaddressed
3  :              Unaddressed          15 :              Unaddressed
4  :Dynamic 100       Static 0         16 :              Unaddressed
5  :Dynamic 300       Static 0         17 :              Unaddressed
6  :              Unaddressed          18 :              Unaddressed
7  :Dynamic 0         Static 3         19 :              Unaddressed
8  :              Unaddressed          20 :              Unaddressed
9  :              Unaddressed          21 :              Unaddressed
10 :              Unaddressed          22 :              Unaddressed
11 :              Unaddressed          23 :              Unaddressed
12 :              Unaddressed          24 :              Unaddressed
                                       AUI:              Unaddressed
A  :              Unaddressed
B  :              Unaddressed

Select [X] Exit to previous menu:
```

The columns on this report have the following values:

- Port number.
- Port—Whether the port is enabled for dynamic learning or is secured.
- Addresses—If it is a single station, this field contains its address; if it is not a single station, this field shows the number of static and dynamic addresses associated with the port.

[X] Exit—Display the Usage Summary Menu.

Exception Statistics Report

To display the Exception Statistics Report (Figure 4-31), enter the **[E] Exception Statistics Report** option from the Usage Summary Menu. This report displays the number of receive errors, transmit errors, and security violations for each port.

Figure 4-31 Exception Statistics Report

```
Catalyst 1900 - Exception Statistics Report (Frame counts)

     Receive   Transmit   Security        Receive   Transmit   Security
     Errors    Errors   Violations       Errors    Errors   Violations
     ---------------------------       ---------------------------
1  :     0         0          0       13 :   0         0          0
2  :     0         0          0       14 :   0         0          0
3  :     0         0          0       15 :   0         0          0
4  :     0         0          0       16 :   0         0          0
5  :     0         0          0       17 :   0         0          0
6  :     0         0          0       18 :   0         0          0
7  :     0         0          0       19 :   0         0          0
8  :     0         0          0       20 :   0         0          0
9  :     0         0          0       21 :   0         0          0
10 :     0         0          0       22 :   0         0          0
11 :     0         0          0       23 :   0         0          0
12 :     0         0          0       24 :   0         0          0
                                     AUI:   0         0          0
A  :     0         0          0
B  :     0         0          0

Select [R] Reset all statistics, or [X] Exit to previous menu:
```

The figures displayed are actually totals of various kinds of errors:

- Receive errors—The combined number of giants and FCS and alignment errors
- Transmit errors—The combined number of excessive deferrals, late collisions, jabber errors, and other transmit errors
- Security violations—The combined number of secure address violations caused by address mismatches or duplications

[R] Reset all statistics—Reset all statistics to zero.

[X] Exit—Display the Usage Summary Menu.

Utilization Statistics Report

To display the Utilization Statistics Report (Figure 4-32), enter the **[U] Utilization Statistics Report** option from the Usage Summary Menu. This report displays the frame-count statistics generated by the switch.

Figure 4-32 Utilization Statistics Report

```
Catalyst 1900 - Utilization Statistics Report (Frame counts)

     Receive    Forward   Transmit       Receive    Forward  Transmit
     ---------------------------- ------------------------------------
1  : 436908     126344   10         13 : 0          0          0
2  : 0          0        0          14 : 0          0          0
3  : 0          0        0          15 : 8          5          685226
4  : 50438      50438    1          16 : 0          0          0
5  : 0          0        0          17 : 685241   161764       8
6  : 685176     161750   8          18 : 169017   104935       0
7  : 0          0        0          19 : 0          0          0
8  : 126599     124963   3          20 : 0          0          0
9  : 0          0        0          21 : 0          0          0
10 : 0          0        0          22 : 86103    86103        4
11 : 0          0        0          23 : 0          0          0
12 : 353676     353676   7          24 : 0          0          685281
                                    AUI: 0          0          0
A  : 0          0        80
B  : 0          0        80

Select [R] Reset all statistics, or [X] Exit to previous menu:
```

Column headings have the following meanings:

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

[R] Reset all statistics—Reset all statistics to zero.

[X] Exit—Display the Usage Summary Menu.

Bandwidth Usage Report

To display the Bandwidth Usage Report (Figure 4-33), enter the **[B] Bandwidth Usage Report** option from the Usage Summary Menu. This report displays the peak bandwidth of the network during a given period of time.

Figure 4-33 Bandwidth Usage Report

```
Catalyst 1900 - Bandwidth Usage Report

--------------------Information----------------

Current bandwidth usage                    0 Mbps
Peak Bandwidth Usage during this interval  0 Mbps
Peak Time recorded since start up          0d 00h 00m 32s

--------------------Settings-----------------

[T] Capture time interval                  24 hour(s)
[R] Reset capture
[X] Exit to previous menu

Enter Selection:
```

[T] Capture time interval—Define the number of hours in which data is collected to calculate bandwidth usage. Figure 1-4 shows the bandwidth associated with each LED. The default is 24 hours.

[R] Reset capture—Enter [**Y**]es to clear the entire peak bandwidth capture table and restart capturing at the current interval. Enter [**N**]o to display the Bandwidth Usage Report.

[X] Exit—Display the Usage Summary Menu.