

Menu-Based Management

This chapter describes the menu console, a menu-drive interface for configuring and monitoring the switch out of band. This chapter provides complete and detailed descriptions of the individual configuration and monitoring options.

Before continuing with this chapter, you should have read the information in the “Overview of the Menu Console” section on page 3-8.

Menu Console Logon Screen

The Menu Console Logon Screen (see Figure 5-1) 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 2-14.)

To log in to the menu console and display the Management Console Main Menu, select the **[M]** option on the Menu Console Logon Screen, and press **Return**.

If a password for the switch has been defined, you are prompted for the password. Enter the password at the prompt, and press **Return**. If you have forgotten the password, you can view the password from the Diagnostic Console - System Debug Interface Menu (see Figure 6-4).

Figure 5-1 **Menu Console Logon Screen**

```
Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc. 1993-1998
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 Configuration
```

```
Enter Selection:
```

Management Console Main Menu

The Management Console Main Menu (see Figure 5-2) is displayed after you log in and select the **[M]** option from the Menu Console Logon Screen. Select an option by entering the letter in brackets next to it. You do not need to press Return.

Figure 5-2 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:
```

Use the **[H]** option to display the online help and to change the expertise level for online prompts.

Console Settings Menu

The Console Settings Menu (see Figure 5-3) is displayed when you select the **[C]** option from the Management Console Main Menu. Use this menu to change the password, set the number of password intrusions allowed, set the default mode for the port status LEDs, and define how long the menu console remains silent after an intrusion.

Figure 5-3 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

[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 menu console becomes quiet for a user-defined length of time before allowing the next log-in attempt. To change the threshold value, enter the new setting. The default setting is 3.

[S] Silent time upon intrusion detection—Enter the number of minutes the menu console is unavailable due to an excessive number of failed attempts to log in. You can specify 0 to 65,500 minutes. The default setting is None (no silent time).

[T] Management console inactivity time-out—Define the length of time the menu console remains idle before it times out. After a timeout, you need to reenter the password. The timeout period is set in seconds; a timeout of zero means the menu console never times out. Enter 0 or a number between 30 and 65,500. The default setting is None (no inactivity timeout).

[D] Default mode of status LED—Select the default mode. The switch returns to this mode 30 seconds after you release the Mode button. You can select **[1] Port Status**, **[2] Utilization**, or **[3] Duplex Status**. The default setting is Port Status.

[M] Modify password—Enter a new password or change a password of four to eight characters. You can use any character found on the keyboard, but *case is not considered*. (If you have a current password, you must enter it before it can be changed.) To erase a password, press the **Backspace** key, and then press **Return**. The default setting is None.

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

System Configuration Menu

The System Configuration Menu (see Figure 5-4) is displayed when you select the [S] option from the Management Console Main Menu. Use this menu to reset the switch and to define the system-wide parameters of the switch.

This section provides additional information about these topics:

- Switching modes
- Broadcast storm control

Figure 5-4 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
```

[N] Name of system—Name of up to 255 characters for the switch.

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

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

[S] Switching mode—Set the switching mode to either FragmentFree (cut-through) or store-and-forward. The default setting is FragmentFree. For additional information, see “Switching Modes” section on page 5-10.

[U] Use of store-and-forward for multicast—Enter **E** (enable) if you want to force store-and-forward mode for multicast frames. The store-and-forward switching mode is always used for broadcast frames. Enter **D** (disable) if you want to use the FragmentFree (cut-through) switching mode. The default setting is Disabled.

[A] Action upon address violation—Define how the switch responds to address violations. Address violations occur when a secured port receives a source address statically assigned to another port or when a secured port tries to learn an address that exceeds its defined maximum number of addresses. Enter one of the following values:

- **[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 reenabled.
- **[I]gnore**—The port status remains unchanged.

[G] Generate alert on address violation—Whether or not the switch changes the port status when an address violation occurs, it can also send an SNMP alert to a management station. Enter **E** to enable or **D** to disable this feature. The default setting is Enabled.

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

[I] Address aging time—Time after which an unused dynamic address is automatically removed. During a topology change, if Port Fast mode is disabled, ports are aged more quickly by using the forward-delay parameter. When the topology stabilizes, this value again takes effect.

Enter from 10 to 1,000,000 seconds (about 11 1/2 days). The default is 300 seconds (5 minutes). This value applies for all dynamic addresses in the switch address table.

[P] Network Port—Define a port as the destination port for all packets with unknown unicast addresses. The switch does not forward unknown unicast addresses to any other ports. The switch does not learn addresses on the network port. This port is usually connected to a legacy network or backbone. A secured port cannot be the network port. If you select a secure port for the network port, you are prompted to disable the security feature. The default setting is None.

A unicast address identifies one unique device on the network. However, if the switch has not received packets from the device for longer than the aging period, the switch removes the address from memory, and the address is then an unknown unicast address. The switch must flood packets destined for the unknown unicast address to ensure the device receives the packet. Once the switch learns the location of the device, this flooding stops.

The Network Port serves only within the bridge groups to which the Network Port is member.

[H] Half duplex back pressure (10BaseT ports)—Enable **[E]** or disable **[D]** the half-duplex back pressure globally on the 10BaseT ports. When enabled, the switch applies back pressure to any half-duplex 10-Mbps ports, if necessary. The default setting is Disabled.

Back pressure ensures the retransmission of incoming packets when a half-duplex port is temporarily unable to receive incoming frames. 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.

[E] Enhanced Congestion Control (10BaseT ports)—Globally enable Enhanced Congestion Control (ECC) on the 10BaseT ports in half-duplex mode.

ECC helps reduce congestion in the switch and helps keep the switch from dropping frames due to full transmit queues. An ECC-enabled port accelerates transmission of frames and empties its queue more quickly.

There are four settings for the ECC option:

- **[1] Adaptive**—If the transmit queue is not full, the port operates under the ECC Disabled setting. If the transmit queue is full, the port uses the ECC Aggressive setting. To use this setting, enter **1**.
- **[2] Disabled** (Default)—The port uses the IEEE 802.3 standard for retransmitting frames. To use this setting, enter **2**.
- **[3] Moderately Aggressive**—The port more aggressively retransmits frames and empties its queue than when set at ECC Disabled. To use this setting, enter **3**.
- **[4] Aggressive**—This is the highest acceleration rate. The port more aggressively retransmits frames and empties its queue than when set at ECC Moderately Aggressive or ECC Disabled. To use this setting, enter **4**.

Note To specify ECC on the 100BaseT ports, use the Port Configuration Menu (100BaseT Ports).

[R] Reset system—Reset the switch. All configured system parameters and static addresses are retained; all dynamic addresses are removed. Enter **Y** (yes) or **N** (no).

[F] Reset with factory defaults—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. Enter **Y** (yes) or **N** (no).

[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.

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

Switching Modes

This section provides additional information about the [S] Switching mode option on the System Configuration Menu.

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. The switch offers the following switching modes:

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

If latency is an issue, use FragmentFree switching.

- The store-and-forward mode stores complete packets and checks for errors before transmission. In this mode, latency is measured as last-bit-received to first-bit-transmitted, or “Last-In, First-Out” (LIFO). This latency does not include the time to receive the entire packet, which can vary, according to packet size. At 100 Mbps, the packet receipt time varies between 51.2 microseconds and 1.2 milliseconds. At 10 Mbps, the packet receipt time varies between 5.12 and 120 microseconds. The store-and-forward mode is always used for broadcast packets and transfers from 10-Mbps to 100-Mbps ports.

Store-and-forward is the most error-free form of switching, but the forwarding latency is higher than FragmentFree (cut-through) switching (see Table 5-1). If you have frame check sequence (FCS) or alignment errors, use the store-and-forward mode so that packets with errors are filtered and not propagated to the rest of the network.

Table 5-1 Switching Latencies

Switching Mode	10 Mbps to 10 Mbps	10 Mbps to 100 Mbps	100 Mbps to 100 Mbps	100 Mbps to 10 Mbps
FragmentFree (cut-through)	70 microsec	–	9 microsec	10 microsec
Store-and-forward ¹	7 microsec	7 microsec	3 microsec	3 microsec

1. Although this table shows store-and-forward experiencing the lowest latency, the figures do not include the time it takes to receive the packet, which varies according to the packet size.

Broadcast Storm Control Menu

The Broadcast Storm Control Menu (see Figure 5-5) is displayed when you select the **[B]** option from the System Configuration Menu. Use this menu to generate SNMP alerts and inhibit the forwarding of broadcast packets when an excessive number (a broadcast storm) arrive from a given port.

A broadcast storm can cause the network to slow down or time out. To avoid this, you can set a threshold for the number of broadcast packets that can be received from a port before forwarding is blocked. You can set a second threshold number to reenable the normal forwarding of broadcast packets.

Broadcast storm control is configured for the switch as a whole, but operates on per-port basis. By default, broadcast storm control does not monitor broadcast traffic and thus does not block traffic or send alerts based on broadcast storms.

Figure 5-5 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—Select the action the switch takes when the broadcast threshold is exceeded. If you choose the block option, the switch drops all broadcast packets received from a port when the number exceeds the broadcast threshold. The switch begins forwarding again when the number drops below the reenable threshold. Enter **B** (block) or **I** (ignore). The default setting is Ignore.

[G] Generate alert when threshold exceeded—Generate SNMP alerts when the broadcast threshold is exceeded. The alert generated is the trapbroadcastStorm. A trap is generated every 30 seconds. Enter **E** (enable) or **D** (disable). The default setting is Disabled.

[T] Broadcast threshold (BCs received / sec)—Set the broadcast threshold, which is the number of packets per second arriving on a port. When this threshold is exceeded, the switch does not forward packets received from the port and can generate an SNMP alert. The default is 500 packets per second. Enter a number between 10 and 14,400.

[R] Broadcast re-enabled threshold—Define when broadcast storm control is automatically disabled. The number of broadcast packets received must drop below this threshold to reenable forwarding. The default is 250 packets per second. Enter a number between 10 and 14,400.

[X] Exit—Display the System Configuration Menu.

Note Only broadcast packets are filtered. Multicast and unicast packets are forwarded normally.

Network Management Menu

The Network Management Menu (see Figure 5-6) is displayed when you select the [N] option from the Management Console Main Menu. Use this menu to display the following menus:

- IP Configuration
- Network Management (SNMP) Configuration
- Spanning Tree Configuration
- CDP Configuration/Status
- Cisco Group Management Protocol (CGMP) Configuration
- HTTP Server Configuration

Figure 5-6 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

[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.

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

IP Configuration Menu

The IP Configuration Menu (see Figure 5-7) is displayed when you select the **[I]** option from the Network Management Menu. Before the switch can be managed in-band, it must have an IP address. Use this menu or DHCP to assign an IP address. You can also use this menu to assign subnet masks and define a default gateway (router) for the switch.

Figure 5-7 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
[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
[X] Exit to previous menu

Enter Selection:
```

[I] IP address—Assign an IP address to the switch. When you assign an IP address, it takes effect immediately.

[S] Subnet mask—If IP subnetting is used, enter a subnet mask (IP address) for the switch. The new value takes effect immediately. If subnetting is not used, the subnet mask is the same as the network mask.

- [G] Default gateway**—Assign a default gateway router address for SNMP management. This is used when the switch is trying to reach a nonlocal IP host.
- [M] IP address of DNS server 1**—Enter the IP address of a domain name system (DNS) server.
- [N] IP address of DNS server 2**—Enter the IP address of a second DNS server.
- [D] Domain name**—Enter a domain name of up to 62 characters.
- [R] Use Routing Information Protocol**—Enable or disable the Routing Information Protocol, which controls automatic discovery of IP gateways. The default setting is enabled.
- [P] Ping**—Ping the IP address or name of an IP device that can be reached from this switch.
- [X] Exit**—Display the Network Management Menu.

Network Management (SNMP) Configuration Menu

The Network Management (SNMP) Configuration Menu (see Figure 5-8) is displayed when you select the [S] option from the Network Management Menu. Use this menu to specify the following:

- Management stations that can set or change the switch MIB objects
- Read and write community strings
- SNMP traps that are enabled and stations that receive them
- Community strings that accompany traps sent by the switch

You can use SNMP management, based on the Catalyst 1900 MIB, to specify management stations authorized to set configuration parameters and to receive traps. Up to four management stations can set MIB objects, and up to three stations can receive traps. If no management station is specified, any SNMP station can set parameters if the correct write community string accompanies the request. However, once a write-manager IP address is defined, only an explicitly specified management station can issue set operations. Once a management station has been assigned, it receives all traps issued by the switch.

Figure 5-8 Network Management (SNMP) Configuration Menu

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

-----Settings-----
[R] READ community string
[W] WRITE community string
[1] 1st WRITE manager name or IP address
[2] 2nd WRITE manager name or IP address
[3] 3rd WRITE manager name or IP address
[4] 4th WRITE manager name or IP address

[F] First TRAP community string
[A] First TRAP manager name or IP address
[S] Second TRAP community string
[B] Second TRAP manager name or IP address
[T] Third TRAP community string
[C] Third TRAP manager name or IP address
[U] Authentication trap generation Enabled
[L] LinkUp/LinkDown trap generation Enabled

-----Actions-----
[X] Exit to previous menu

Enter Selection:
```

[R] READ community string—Define the SNMP agent Get community string. Enter a string of up to 32 characters. The default is Public.

[W] WRITE community string—Define a write community string for the switch. Enter up to 32 characters. The default is Private.

[1–4] WRITE manager name or IP address—Use the write manager name or IP address [1–4] options to enter the IP addresses of stations authorized to issue write requests to the switch. You can specify the name of the write manager if the switch is connected to a domain name server. To remove an entry, enter **0. 0. 0. 0**.

[F, S, T] TRAP community string and **[A, B, C] TRAP Manager name or IP address**—Use the trap community string [F, S, T] options and trap manager name or IP address [A, B, C] options to define up to three trap clients and their accompanying community strings.

A trap manager, or trap client, is a management workstation configured to receive and process traps. You can specify up to three trap managers with separate community strings. At least one trap manager must be defined before traps are sent.

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

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

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

[U] Authentication trap generation—Enable [E] or disable [D] authentication traps that alert a management station of SNMP requests not accompanied by a valid community string. Even if this parameter is set, no trap is generated if no trap manager addresses have been specified. The default setting is Enabled.

[L] LinkUp/LinkDown trap generation—Enable [E] or disable [D] the linkUp/linkDown trap. The default setting is Enabled. The switch generates the linkDown trap whenever a port changes to a suspended or disabled state due to any of the following:

- Spanning-Tree Protocol action
- Secure address violation (address mismatch or duplication)

- Network connection error (loss of linkbeat or jabber error)
- Management intervention

The linkUp trap is generated whenever a port changes to the enabled state due to the following:

- Presence of linkbeat
- Spanning-Tree Protocol action
- Management intervention
- Recovery from an address violation or any other error

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

After you have specified the management workstation(s) to receive traps, the switch generates, by default, the traps in the following list:

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

[X] Exit—display the Network Management Menu.

Spanning Tree Configuration Menu

The Spanning Tree Configuration Menu (see Figure 5-9) is displayed when you select the **[B]** option from the Network Management Menu. Use this menu to display and configure the Spanning-Tree Protocol parameters defined for the switch.

The Information section represents parameters controlled by Spanning-Tree Protocol operation as influenced by other bridges on the network. The Settings section defines Spanning-Tree Protocol parameters that are global to this bridge. For more information, read the “Spanning-Tree Protocol” section on page 5-22.

Note The Port Fast mode option, recommended for end-station attachments only, brings a port from a blocking state directly to a forwarding state. However, during system startup, the Spanning-Tree Protocol first ensures no temporary loops are formed. This discovery takes approximately 30 seconds to complete, and no packets are forwarded. Ports with Port Fast mode enabled then change to the forwarding state with no delay. See the “Port Configuration Menu” section on page 5-30 for configuration instructions.

Figure 5-9 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:
```

Table 5-2 describes the information fields on this menu. These parameters apply to the spanning tree of bridge group1 (the management bridge group):

Table 5-2 Spanning Tree Configuration Menu Field Descriptions

Field	Description
Bridge ID	Unique hexadecimal ID number has a bridge priority and a unique MAC address.
Number of member ports	Number of ports configured with Spanning-Tree Protocol.
Designated root	ID of the bridge identified as the root by the Spanning-Tree Protocol.
Root port	Port on this bridge with the lowest-cost path to the root bridge. This option identifies the port through which the path to the root bridge is established. N/A is displayed when Spanning-Tree Protocol is disabled or when this bridge is the root bridge.
Max age	Number of seconds a bridge waits without receiving Spanning-Tree Protocol configuration messages before attempting a reconfiguration.
Root path cost	Cost of the path from this bridge to the root bridge shown in Designated root. It equals the path cost parameters held for the root port. When this switch is the root, the root path cost is zero.
Forward delay	Number of seconds before a port changes from its Spanning-Tree Protocol learning and listening states to a forwarding state. This is necessary because every bridge on the network ensures no loop is formed before allowing the port to forward packets.
Hello time	Number of seconds between the transmission of Spanning-Tree Protocol configuration messages. All bridges send configuration messages during reconfiguration to elect the designated root bridge. After the topology is stabilized, only designated bridges send configuration messages.
Topology Changes	Number of bridge topology changes experienced by this bridge. A topology change occurs as ports on this bridge change from a nonforwarding to forwarding state or when a new root is selected.
Last TopChange	Number of days (d), hours (h), minutes (m), and seconds (s) since the last topology change.

[S] Spanning-Tree Algorithm and Protocol—Enable **[E]** or disable **[D]** the Spanning-Tree Protocol, an IEEE 802.1D standard to ensure a loop-free configuration in the bridge topology. When Spanning-Tree Protocol is enabled, redundant ports are kept in standby (suspended) status and are enabled when needed. For additional information about this option, see the “Spanning-Tree Protocol” section on page 5-22. The default setting is Enabled.

[B] Bridge priority—Value (0 through 65535) used in determining the identity of the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. The default is 32768.

[M] Max age when operating as root—Number of seconds (6 to 40) to be used as the Max age interval when this switch becomes the root bridge. After this period expires, other bridges recognize that the root has not sent a configuration message, and a new root is selected. The default is 20.

[H] Hello time when operating as root—Number of seconds (1 to 10) when this switch becomes the root bridge. The default is 2.

[F] Forward delay when operating as root—Number of seconds (4 to 30) to be used as the forward-delay interval when this switch becomes the root bridge. The default is 15 seconds.

Note Spanning-Tree Protocol also uses this value to accelerate address aging when the spanning tree is reconfigured. See the following “Spanning-Tree Protocol” section on page 5-22 for more information.

[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.

Spanning-Tree Protocol

This section provides additional information about the **[S]** Spanning-Tree Algorithm and Protocol option.

Spanning-Tree Protocol is a standard for maintaining a network of multiple bridges or switches. As part of the IEEE 802.1d standard, Spanning-Tree Protocol interoperates with compliant bridges and switches from other vendors. When the topology changes, it transparently reconfigures bridges to avoid the creation of loops and to establish redundant paths in the event of lost connections.

All ports on the switch support Spanning-Tree Protocol, and management of Spanning-Tree Protocol is through the standard Bridge MIB.

- Using Spanning-Tree Protocol to support redundant connectivity—You can create a redundant backbone with Spanning-Tree Protocol by connecting two of the ports on a switch to another device or to two different devices. Spanning-Tree Protocol automatically disables one port but enables it if the other port is lost. If one link is high-speed and the other low-speed, the low-speed link is always disabled. If the speed of the two links is the same, the port priority and port ID are added together, and the link with the lowest value is disabled.
- Spanning-Tree Protocol and 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 were unreachable for 5 minutes or more, the address-aging time is accelerated so that station addresses can be dropped from the address table and then relearned. The accelerated aging is the same as the forward-delay parameter value when Spanning-Tree Protocol reconfigures. You can define the forward-delay parameter from the **[F]** Forward delay option on the Spanning Tree Configuration Menu.

CDP Configuration/Status Menu

The CDP Configuration/Status Menu (see Figure 5-10) is displayed when you select the [C] option from the Network Management Menu. Use this menu to enable the Cisco Discovery Protocol (CDP) on some or all of the switch ports. You can also use this menu to set the timing for transmission of CDP messages.

CDP provides network managers with an accurate picture of the network at any time. By gathering information about the types of devices in the network, the links between those devices, and the number of interfaces within each device, CDP enables network management applications to display a topological map of the network. Detailed information about the connections between devices is also available.

Figure 5-10 CDP Configuration/Status Menu

```
Catalyst 1900 - CDP Configuration/Status

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

-----Settings-----

[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:
```

[H] Hold Time—Set the number of seconds that a neighboring device retains the CDP neighbor information received from this switch. If a neighboring device does not receive a CDP message before this hold time expires, the neighboring device drops this switch as a neighbor. Enter a number between 5 and 255. The default setting is 180.

[T] Transmission Interval—Set the number of seconds between transmissions of CDP messages. Enter a number between 5 and 900. The default setting is 60.

[E] Enable CDP on Port(s)—Enable CDP on one or more ports. You can separate the port numbers with a hyphen to create a range or can use commas or spaces between port numbers. Enter the high-speed port: A or B. The word ALL creates a list of all the switch ports. Enter port numbers according to these conventions. The default settings for all ports is Enabled.

[D] Disable CDP on Port(s)—Disable CDP on one or more ports. Enter the port numbers according to the conventions described in the previous paragraph.

[S] Show Neighbor—Display the information available about neighboring devices (see Figure 5-11). The first two lines in the display define the abbreviations used.

Figure 5-11 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    192.9.200.192    4          TS         cisco 1900    3
00C01D80727     192.9.200.221    6          TS         cisco 1900    10

Press any key to continue.
```

[X] Exit—Display the Network Management Menu.

Cisco Group Management Protocol

The Cisco Group Management Protocol (CGMP) Configuration Menu (see Figure 5-12) is displayed when you select the **[G]** option from the Network Management Menu. CGMP is enabled by default. Use this menu to enter the number of seconds the switch waits for keepalive messages before deleting CGMP-learned multicast groups, to enable or disable CGMP, or to list IP multicast addresses.

Figure 5-12 Cisco Group Management Protocol (CGMP) Configuration Menu

```
Catalyst 1900 - Cisco Group Management Protocol (CGMP) Configuration
-----Settings-----
[H] Router Hold Time (secs)           300
[C] CGMP                               Enabled

-----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. The default setting 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 advertising message. When the last CGMP-capable router goes down, the switch discards the multicast-group information from the router.

[C] CGMP—Enable **[E]** or disable **[D]** CGMP. The default setting is Enabled.

CGMP manages multicast traffic by allowing directed switching of IP multicast traffic within a network. CGMP offers the following benefits:

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

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

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

For additional information about CGMP and multicast addresses, see the “IP Multicast Addresses” section on page 5-27, “Joining a Multicast Group” section on page 5-27, and “Leaving a Multicast Group” section on page 5-28.

[L] List IP multicast addresses—List the IP multicast addresses currently being handled by CGMP.

If you have configured bridge groups, the bridge group number is not displayed. For more information on bridge groups, see the “Bridge Group Configuration Menu” section on page 5-47.

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



Caution The **[R]** option is used when recovering from unexpected situations.

[X] Exit—Display the Network Management Menu.

IP Multicast Addresses

CGMP works in conjunction with IGMP messages to dynamically configure the switch ports so that IP multicast traffic is forwarded only to those ports associated with IP multicast hosts.

CGMP software components run on both the router and the switch. A CGMP-capable IP multicast router sees all IGMP packets and therefore can inform the switch when specific hosts join or leave IP multicast groups. When the CGMP-capable router receives an IGMP control packet, it creates a CGMP packet with the request type (either join or leave), the multicast group address, and the actual MAC address of the host. The router then sends the CGMP packet to a well-known address which Catalyst 1900 switches monitor. When a switch receives the CGMP packet, the switch interprets the packet and modifies the forwarding behavior of the multicast group. From then on, this multicast traffic is sent only to ports associated with the appropriate IP multicast clients. This process is done automatically, without user intervention.

User-specified multicast group settings are static, whereas multicast groups learned through CGMP are dynamic. While CGMP is active, you cannot manually configure a multicast MAC address that corresponds with an IP multicast group.

Joining a Multicast Group

When a particular host attempts to join an IP multicast group, it sends an IGMP join message specifying its MAC address and the IP multicast group it is attempting to join. The CGMP-capable router then builds a CGMP join message and multicasts the join message to the well-known address which the switch monitors. Upon receipt of the join message, each switch searches its forwarding table for the MAC address of the sending host. If a switch finds the host MAC address in its forwarding table associating the MAC address with a nontrunking port, the switch creates a multicast forwarding entry in the forwarding table. The host associated with that port then receives multicast traffic for that multicast group. In this way, the forwarding engine automatically learns the MAC addresses and port numbers of the IP multicast hosts.

Leaving a Multicast Group

The multicast router sends periodic multicast-group queries. If a host should remain in a multicast group, it responds to the query from the router. In this case, the router does nothing. If a host should not remain in the multicast group, it does not respond to the router query. If, after a number of queries, the router receives no reports from any host in a multicast group, the router sends a CGMP command to the switch, telling it to remove the multicast group from its forwarding tables.

Note If there are other hosts in the same multicast group and they *do* respond to the multicast-group query, the router does not tell the switch to remove the group from its forwarding tables. The router does not remove a multicast group from the switch forwarding tables until all the hosts in the group have left the group.

HTTP Server Configuration Menu

The HTTP Server Configuration Menu (see Figure 5-13) is displayed when you select the **[H]** option from the Network Management Menu. Use this menu to access the switch through one of its Ethernet 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 you are connected to. Changes to the switch IP information should be done with care.

Figure 5-13 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—Enable **[E]** or disable **[D]** the HTTP server on the switch. The default setting is Enabled.

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

[X] Exit—Display the Network Management Menu.

Port Configuration Menu

When you select the **[P]** 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, select 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 5-14 is displayed. If you select a 100BaseT port (ports Ax or Bx), the Port Configuration Menu (100BaseT Ports) in Figure 5-15 is displayed.

Use the Port Configuration Menu to display the status of a port, enter a port description, change the port status, and define various Spanning-Tree Protocol parameters.

Use the Port Configuration Menu to display and change the status of a port, enter a port description, and define various performance (such as duplex mode and ECC) and Spanning-Tree Protocol parameters. Table 5-3 describes the possible states for the ports.

Table 5-3 Spanning-Tree Protocol States

State	Description
Blocking	Port is not participating in the frame-forwarding process and is not learning new addresses.
Listening	The same as blocking, but the switch is actively trying to bring the port into the forwarding state. The port is not learning addresses.
Learning	Port is not forwarding frames but is learning addresses. The switch is actively trying to bring the port into the forwarding state.
Forwarding	Port is forwarding frames and learning addresses.
Disabled	Port has been removed from operation. Administrative intervention is required to enable the port.

Figure 5-14 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 5-15 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:
```

The following descriptions are common among the Port Configuration Menus for the 10BaseT and 100BaseT ports:

The Forward Transitions field displays the number of times the Spanning-Tree Protocol state for this port has changed from listening or learning to forwarding.

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

[S] Status of port—Enable **[E]** or disable **[D]** a port. Port status is a system-wide indicator of the state of a port. Security violations, management intervention, or actions of the Spanning-Tree Protocol can change the port status. Each port is always in one of the states listed in Table 5-4.

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. If a linkbeat returns, for example, a port suspended for no linkbeat returns to the enabled state.

Table 5-4 Port Status Definitions (Menu Console)

Port Status	Definition
Enabled	Normal operation. Port can transmit and receive.
Disabled-mgmt	Disabled by explicit management action. If the port is disabled, you must manually reenale it.
Suspended-no-linkbeat	Suspended due to the absence of a linkbeat. This is usually because the attached station is disconnected or powered-down. Port automatically returns to enabled state when the cause of the suspension is removed.
Suspended-jabber	Suspended because attached station is jabbering. Port automatically returns to enabled state when the cause of the suspension is removed.
Suspended-violation	Suspended due to address violation. Port automatically returns to enabled state when the cause of the suspension is removed.
Disabled-self-test	Disabled because port failed self-test. Port must be manually returned to enabled state.
Disabled-violation	Disabled due to address violation. Port must be manually returned to enabled state.
Reset	Port is resetting.

[F] Full duplex (10BaseT ports)—Enable **[E]** or disable **[D]** full-duplex transmission on the 10BaseT ports. The default setting is half-duplex mode (full-duplex disabled). Full-duplex flow control is not supported on the 10BaseT ports.

Full-duplex operation is simultaneous transmission of data in both directions across a link. For example, 10BaseTX ports operating in full-duplex mode can provide up to 20 Mbps of bandwidth across the switched link.

You can use full-duplex connections (either 10 Mbps or 100 Mbps) to enhance transmission speeds between other switches or routers that support full-duplex operation. A likely full-duplex scenario would be to connect a 100BaseT port to a server with a 100BaseT adapter configured for full-duplex operation.

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

Note To specify full-duplex operation on the 100BaseT ports, use the Port Configuration Menu (100BaseT Ports).

[I] Port priority—Define which port is to remain enabled by Spanning-Tree Protocol if two ports form a loop. Enter a number from 0 to 255. The default setting is 128.

[C] Path cost—Define the Spanning-Tree Protocol path cost of the port. The default value is inversely proportional to the LAN speed of the network interface at the port. A high path cost means the port has low bandwidth and should not be used, if possible. The default is 1000/LAN-speed-in-Mbps. The path cost of 100-Mbps ports is thus 10, and the path cost of 10-Mbps ports is 100. This option also affects which port is to remain enabled by Spanning-Tree Protocol if another bridge device forms a loop with the switch. Enter a value between 1 and 65535. The default setting for the 10BaseT ports is 100. The default setting for the 100BaseT ports is 10.

[H] Port Fast mode—Accelerate the time it takes for Spanning-Tree Protocol to bring a port into the forwarding state. Port Fast-enabled ports are used for end-station attachments only. The Port Fast option is a simplified version of the Spanning-Tree Protocol that bypasses the normal pre-forwarding spanning-tree states, more quickly bringing ports into the forwarding states. Port Fast is an option that you can enable on a per-port basis. Enter **E** (enable) or **D** (disable). The default setting for the 10BaseT ports is Enabled. The default setting for the 100BaseT ports is Disabled.

Note When the switch is powered up, the forwarding state, even if the 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, ports with Port Fast mode enabled transition directly from the blocking state to the forwarding state.

[E] Enhanced congestion control (100BaseT ports)—Enable Enhanced Congestion Control (ECC) on a port-by-port basis for the 100BaseT ports. The ECC option applies only when the ports are operating in half-duplex mode.

ECC helps reduce congestion in the switch and helps keep the switch from dropping frames due to full transmit queues. An ECC-enabled port uses a modified backoff algorithm to accelerate transmission of frames and empty its queue more quickly.

At the prompt, select one of the settings:

- **[1] Adaptive**—If the transmit queue of the port is not full, the port operates under the ECC Disabled setting. If the transmit queue is full, the port uses the ECC Aggressive setting. To use this setting, enter **1**.
- **[2] Disabled (Default)**—The port uses the standard IEEE 802.3 backoff algorithm for retransmitting frames. To use this setting, enter **2**.
- **[3] Moderately Aggressive**—The port uses a modified backoff algorithm to more aggressively retransmit frames and empty its queue than when set at ECC Disabled. To use this setting, enter **3**.
- **[4] Aggressive**—This is the highest acceleration rate configurable for the ECC option. The port uses a modified backoff algorithm to more aggressively retransmit frames and empty its queue than when set at ECC Moderately Aggressive or ECC Disabled. To use this setting, enter **4**.

To specify ECC on the 10BaseT ports, use the System Configuration Menu described in the “System Configuration Menu” section on page 5-6.

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

[F] Full-duplex/Flow Control (100BaseT ports)—Assign, on a port-by-port basis, full-duplex operation on the 100BaseTX and 100BaseFX ports. At the prompt, select one of the settings: **[1] Full duplex**, **[2] Half duplex**, **[3] Full duplex with flow control**, or **[4] Auto-negotiate**. The default setting of the 100BaseTX ports is auto-negotiate. The default setting of the 100BaseFX switched port is half-duplex mode (see the “Flow Control” section on page 5-36 for more information about this standard).

Note To specify duplex operation on the switched 10BaseT ports, use the Port Configuration Menu (10BaseT Ports).

Flow Control

All 100BaseT ports operating in full-duplex mode support the IEEE 802.3x implementation of port-based flow control. When flow control is enabled, the switch responds to pause-control frames received from other connected devices. 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 the transmission of frames through the affected 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 The 10-Mbps ports support half-duplex back pressure. To specify back pressure on the 10-Mbps ports, use the System Configuration 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 currently 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.

Port Addressing Menu

When you select the [A] 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, select the specific port that you want to configure. The Port Addressing Menu (see Figure 5-16) is then displayed. Use the Port Addressing Menu to configure address security of a port and to define static unicast and multicast addresses. You can also specify how a port filters and forwards unmatched unicast addresses and nonregistered multicast addresses. Although multicast address registrations are configured elsewhere, you can use this menu to specify additional source-port filtering on the multicast addresses.

Additional information about address learning, flooding controls, and securing ports is provided later in this section.

Figure 5-16 Port Addressing Menu

```
Catalyst 1900 - Port 1 Addressing

Address : Static      00-00-00-00-00-1B

----- Settings -----
[T] Address table size                Unrestricted
[S] Addressing security                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 zero.
- **Static addresses**—The current number of unicast addresses that have been assigned to this port.

For more information about address learning, see the “Address Learning” section on page 5-40.

[T] Address Table Size—Define the size of the address table for a secured port. Enter a number between 1 and 132.

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

[S] Addressing security—Secure a port. Enter **E** (enable) or **D** (disable). The default setting is Disabled.

Alerts can be generated when a secured port attempts to learn new addresses and its address table is full. The port can be disabled or suspended due to such address violations. See the “Securing Ports” section on page 5-42 for more information.

This option must be disabled for network ports.

[U] Flood unknown unicasts—Enable **[E]** or disable **[D]** the forwarding of unknown unicasts to this port. When a frame with an unrecognized unicast destination address is received on any port, the default action forwards the packet to all enabled ports. For more information, see the “Flooding Controls” section on page 5-40. The default setting is Enabled.

[M] Flood unregistered multicasts—Enable **[E]** or disable **[D]** the forwarding of unregistered multicast addresses to this port. The default setting is Enabled. When a frame with an unregistered multicast destination address is received on any port, the default action forwards the packet to all enabled ports. For more information, see the “Flooding Controls” section on page 5-40.

This option must be disabled for network ports.

[A] Add a static address—If there is room in the port address table, use this option to add a static unicast address. If the address table is full, an error message is generated. You can change the size of the address table with the **[T]** Address table size option.

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.

[D] Define a restricted static address—Enter the restricted static unicast or multicast address. Packets with static addresses are usually accepted from any source port. However, a restricted static address, which corresponds to IEEE 802.1d source port filtering, is accompanied by a list of ports that are allowed to send frames to this address and port.

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.

[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.

[R] Remove all addresses—Remove all dynamic and static addresses currently associated with the port. Enter **Y** (yes) or **N** (no) at the confirmation prompt.

[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 currently 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.

Address Learning

This section provides additional information for understanding and using the options on the Port Addressing Menu.

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

You can manually enter addresses into the address table, including static addresses. Because static addresses do not age, you must manually remove them. Static addressing also allows for a measure of security in that access to a port can be restricted. See the “Securing Ports” section on page 5-42 for more information.

Flooding Controls

This section provides information about using the flooding and addressing options on the Port Addressing Menu.

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

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

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

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

In another example, when the switch receives a multicast packet, you can use the Multicast Registration Menu or SNMP to register multicast addresses and specify to which ports these packets are to be forwarded. You can also disable the normal flooding of unregistered multicast packets on a per-port basis. Besides reducing unnecessary traffic, these features open up the possibility of using multicast packets for dedicated groupcast applications such as broadcast video. For more information about using the Multicast Registration Menu, see the “Multicast Registration Menu” section on page 5-49.

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

Securing Ports

This section provides additional information for using the [S] Addressing security option on the Port Addressing Menu.

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

The number of devices on a secured port can range from 1 to 132. The addresses for the devices on a secure port are statically assigned by an administrator or *sticky-learned*. Sticky-learning takes place when the address table for a secured port does not contain a full complement of static addresses. The port sticky-learns the source address of incoming packets and automatically assigns them as static addresses.

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

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

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

Port Statistics Report

When you select the **[D]** 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, select the specific port for which you want to display the statistics and errors: If you select a switched 10BaseT port (ports 1x through 24x, AUI) or port A or B, the Detailed Port Statistics Report in Figure 5-17 is displayed.

The Detailed Port Statistics Report displays the frame transmit and receive statistics captured by the switch. The statistics and errors can be displayed for all ports on a per-port basis.

If you are using VT100 terminal emulation, the statistics displays are refreshed every 5 seconds. If you are connected to the menu console via a modem running at less than 2400 baud, the statistics displays are refreshed every 8 seconds.

Figure 5-17 is an example statistics report for a 10BaseT port. It is similar to the report for the 100BaseT ports.

Figure 5-17 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:

Port statistics could reveal performance or connectivity problems, particularly those under the Errors heading (Table 5-5). 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

Table 5-5 Error Descriptions on the Detailed Port Statistics Report Screen

Heading Error	Description
FCS errors	A count 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	A count 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	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Address violations	The 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	The 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	A count of frames for which transmission is deferred for an excessive period of time.
Jabber errors	The 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—Clear the port statistics by entering **Y** (yes). 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 currently 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 Monitoring Configuration Menu (see Figure 5-18) is displayed when you select the [M] option from the Management Console Main Menu. Use this menu to do the following:

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

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

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

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

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

Figure 5-18 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:
```

[C] Capturing frames to the Monitor—Enable **[E]** or disable **[D]** frame capturing. The default setting is Disabled.

[M] Monitor port assignment—Specify the number of the port where captured frames are to be sent. The port capture list can include any number of the ports, from none to all 15 or 27 ports. The default is None.

[A] Add ports to capture list—Add port numbers to the capture list.

[D] Delete ports from capture list—Delete port numbers from the capture list. Enter the port numbers that you want to delete.

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

Bridge Group Configuration Menu

The Bridge Group Configuration Menu (see Figure 5-19) is displayed when you select the **[B]** option from the Management Console Main Menu. The bridge group feature 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. A port must always be a member of at least one bridge group and can belong to more than one bridge group if the Overlapping Bridge Groups option is enabled.

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.

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

Figure 5-19 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—Enable **[E]** or disable **[D]** overlapping of bridge groups. If this option is enabled, ports can then belong to more than one bridge group. This option cannot be disabled if any port belongs to multiple bridge groups. The default setting is Disabled.

[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 Overlapping Bridge Groups 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 Overlapping Bridge Groups 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 Overlapping Bridge Groups option is enabled.

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

Multicast Registration Menu

The Multicast Registration Menu (see Figure 5-20) is displayed when you select the **[R]** option from the Management Console Main Menu. By default, all multicast packets are forwarded to all ports of the switch. However, you can use this menu to register multicast addresses and list the ports these packets are to be forwarded to. Because these packets are then *not* forwarded to other ports, this reduces the amount of flooding performed by the switch.

You can also disable the normal flooding of unregistered multicast packets on a per-port basis. Besides reducing unnecessary traffic, these features open up the possibility of using multicast packets for dedicated groupcast applications such as broadcast video.

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

Figure 5-20 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:
```

[R] Register a multicast address—Register a multicast address. You can enter both the address and the ports to which frames destined for this address are to be forwarded. 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.

[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.

See the “Flooding Controls” section on page 5-40 for more information.

[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

The Firmware Configuration Menu (see Figure 5-21) is displayed when you select the [F] option from the Management Console Main Menu. Use this menu to display the firmware version used by the switch and to perform firmware upgrades.

Figure 5-21 Firmware Configuration Menu

```
Catalyst 1900 - Firmware Configuration

-----System Information-----
FLASH: 1024K bytes
V8.00.00 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      Enabled

-----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] Server: IP address of TFTP server—Enter the IP address of the TFTP server where the upgrade file is located.

[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—Enable **[E]** or disable **[D]** the switch from accepting an upgrade from another host on the network. To prevent unauthorized upgrades, use the Disabled setting. The default setting is Enabled.

[U] System XMODEM upgrade—Use this option to upgrade the firmware using a modem. Enter **N** to return to the Firmware Upgrade Menu or **Y** to begin the download. 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 Logon Security Menu is displayed.

[T] System TFTP upgrade—Upgrade the firmware 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.

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

Downloading the Switch Firmware from a TFTP Server

When you upgrade the firmware, download the upgrade file into a temporary area. After 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.

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

- Step 1** From the Firmware Configuration Menu, select the **[S]** option, and enter the IP address or name of the TFTP server where the upgrade file is located.
- Step 2** Select the **[F]** option from the menu, and enter the name of the upgrade file.
- Step 3** Select the **[T]** option from the menu to initiate the TFTP download.
The switch contacts the server to download the upgrade file to the switch.
- Step 4** 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`.

During the download of the upgrade file, the switch does not respond to commands for approximately 1 minute. This is normal and correct. When the download is complete, the switch resets and begins using the new firmware.



Caution If you interrupt the download by turning the switch off and on, the firmware could be corrupted. If this happens, restart the firmware following the procedure described in the “Using the Diagnostic Console” section on page 6-6.

Note You can also initiate a TFTP download by setting the `upgradeTFTPInitiate` MIB object.

Downloading the Switch Firmware from a TFTP Client

When you upgrade the firmware, download the upgrade file into a temporary area. After 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.

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

- Step 1** From the TFTP client workstation, establish a TFTP session with the IP address assigned to the switch.
- Step 2** Ensure that the TFTP client is in binary transfer mode.
- Step 3** Use the appropriate command (such as, **put** *upgrade_filename*) to download the upgrade file from the client workstation to the switch.
- Step 4** 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*.

During the download of the upgrade file, the switch does not respond to commands for approximately 1 minute. This is normal and correct. When the download is complete, the switch resets and begins using the new firmware.



Caution If you interrupt the download by turning the switch off and on, the firmware could be corrupted. If this happens, restart the firmware following the procedure described in the “Using the Diagnostic Console” section on page 6-6.

Downloading the Switch Firmware with the XMODEM Protocol

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

When you upgrade the firmware, download the upgrade file into a temporary area. After 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.

To download the switch firmware via XMODEM, follow these steps:

- Step 1** 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 2** From the Firmware Configuration Menu, select the [U] option to use the XMODEM protocol to download the upgrade file.
- Step 3** At the prompt, select Y to start the download.

During the download of the upgrade file, the switch does not respond to commands for approximately 1 minute. This is normal and correct. When the download is complete, the switch resets and begins using the new firmware.



Caution If you interrupt the download by turning the switch off and on, the firmware could be corrupted. If this happens, restart the firmware following the procedure described in the “Using the Diagnostic Console” section on page 6-6.

RS-232 Interface Configuration Menu

The RS-232 Port Configuration Menu (see Figure 5-22) is displayed when you select the **[I]** option from the Management Console Main Menu. Use this menu to define the physical characteristics of the console port—baud rate, stop bits, and the like—and call features such as the time delay between outgoing calls.

Figure 5-22 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 select 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 setting is 9600.

[D] Data bits—Enter the data bits value for the console port. Valid values are 7 and 8. The default setting is 8.

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

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

[M] Match remote baud rate—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 **E** (enable) or **D** (disable). The default setting is Enabled.

[A] Auto answer—Enable the auto-answer feature. Enter **E** (enable) or **D** (disable). The default setting is Enabled.

[N] Number for dial-out connection—Enter the phone number 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.

Enter up to 48 characters. 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 setting 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 press **G**. Press **C** to cancel the session and to return to the previous settings.

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

Usage Summary Menu

The Usage Summary Menu (see Figure 5-23) is displayed when you select the [U] option from the Management Console Main Menu. Use this menu to display summaries of network statistics for all ports. These reports are read-only.

If you are using VT100 terminal emulation, the statistics displays are refreshed every 5 seconds. If you are connected to the menu 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 5-23 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:
```

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

Port Status Report

The Port Status Report (see Figure 5-24) is displayed when you select the **[P]** 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 5-30.

Figure 5-24 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

The Port Addressing Report (see Figure 5-25) is displayed when you select the **[A]** 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 5-25 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

The Exception Statistics Report (see Figure 5-26) is displayed when you select the [E] option from the Usage Summary Menu. This report displays the number of receive errors, transmit errors, and security violations for each port.

Figure 5-26 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

The Utilization Statistics Report (see Figure 5-27) is displayed when you select the [U] option from the Usage Summary Menu. This report displays the frame-count statistics generated by the switch.

Figure 5-27 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

The Bandwidth Usage Report (see Figure 5-28) is displayed when you select the **[B]** option from the Usage Summary Menu. This report displays the peak bandwidth of the network during a given period of time.

Figure 5-28 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. Table 1-6 in the “Port Status LEDs, Port Mode LED, and Mode Button” section on page 1-7 shows the bandwidth associated with each LED. The default setting is 24 hours.

[R] Reset capture—Clear the entire peak bandwidth capture table and restart capturing at the current interval. Enter **Y** (yes) or **N** (no).

[X] Exit—Display the Usage Summary Menu.

